# MiVoice 5300 IP/Digital Phones
# Mitel 6700 and 6800 SIP Phones
# MiVoice 6900 IP Phones

03/2018
AMT/PTD/TR/0014/13/1/EN

INSTALLATION MANUAL - COMPLETE VERSION

Mitel®

**NOTICE**

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®).

The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries.

Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

©Copyright 2015, Mitel Networks Corporation. All rights reserved.

Mitel® is a registered trademark of Mitel Networks Corporation.

Any reference to third party trademarks is for reference only and Mitel makes no representation of ownership of these trademarks.

# CONTENTS


**1 ABOUT THIS DOCUMENT ..... 15**

1.1 PURPOSE OF THIS DOCUMENT ..... 15
1.2 TARGET AUDIENCE OF THIS DOCUMENT ..... 15
1.3 SCOPE OF THIS DOCUMENT ..... 15
1.4 TERMINOLOGY ..... 16
1.4.1 TERMS AND EXPRESSIONS ..... 16
1.4.2 ABBREVIATIONS ..... 17
1.5 REFERENCE DOCUMENTS ..... 18
1.5.1 TERMINAL RELATED DOCUMENTS ..... 18
1.5.2 SYSTEM RELATED DOCUMENTS ..... 19

**2 MIVOICE 5300 IP PHONES ..... 21**

2.1 MIVOICE 5360 IP PHONES ..... 21
2.1.1 DESCRIPTION OF MIVOICE 5360 IP PHONE ..... 21
2.1.2 SALES CODE FOR MIVOICE 5360 IP PHONE ..... 21
2.2 MIVOICE 5361 IP PHONES ..... 22
2.2.1 DESCRIPTION OF MIVOICE 5361 IP PHONE ..... 22
2.2.2 SALES CODE FOR MIVOICE 5361 IP PHONE ..... 22
2.3 MIVOICE 5370 IP PHONES ..... 22
2.3.1 DESCRIPTION OF MIVOICE 5370 IP PHONE ..... 22
2.3.2 SALES CODE FOR MIVOICE 5370 IP PHONE ..... 22
2.4 MIVOICE 5380 IP PHONES ..... 23
2.4.1 DESCRIPTION OF MIVOICE 5380 IP PHONE ..... 23
2.4.2 SALES CODE FOR MIVOICE 5380 IP PHONE ..... 23
2.5 MIVOICE 5300 IP PHONE CONNECTIONS ..... 24
2.5.1 REMOTE POWER SUPPLY TO MIVOICE 5300 IP PHONES (POE) ..... 24
2.5.2 HEADSETS COMPATIBLE WITH MIVOICE 5370 DIGITAL PHONE AND 5380 IP PHONE ..... 25
2.6 ELECTRICAL POWER CONSUMPTION OF MIVOICE 5300 IP PHONE ..... 27
2.7 MIVOICE M530 EXTENSION MODULE ..... 27
2.7.1 CHARACTERISTICS OF THE MIVOICE M530 EXTENSION MODULE ..... 27
2.8 OPTIONAL ACCESSORIES ..... 28
2.9 TELEPHONY FEATURES OF MIVOICE 5300 IP PHONE ..... 28
2.10 MIVOICE 5000 ARCHITECTURES WITH MIVOICE 5300 IP PHONE ..... 29
2.11 MIVOICE 5300 IP PHONE CONFIGURATION MODES ..... 30
2.11.1 CONNECTING THE DATA SWITCH ..... 31
2.12 CONFIGURING MIVOICE 5300 IP PHONES FOR DUAL HOMING ..... 32
2.13 CONFIGURING MIVOICE 5300 IP PHONE FOR THE MD5 AUTHENTICATION FUNCTION ..... 33
2.13.1 CONFIGURING THE MD5 PASSWORD IN THE IPBX ..... 33
2.13.2 CONFIGURING THE MD5 PASSWORD MANUALLY IN MIVOICE 5300 IP PHONES ..... 34
2.13.3 AUTOMATIC CONFIGURATION OF THE MD5 PASSWORD IN THE MIVOICE 5300 IP PHONES ..... 35
2.14 CONFIGURING MIVOICE 5300 IP PHONES IN THE 802.1X ENVIRONMENT ..... 36
2.14.1 WORKING PRINCIPLE: ..... 36
2.14.2 CONFIGURING THE 802.1X AUTHENTICATION PARAMETERS OF MIVOICE 5300 IP PHONES ..... 37
2.14.3 MIVOICE 5300 IP PHONE AUTHENTICATION PROCEDURES ..... 37
2.14.4 SWITCH BEHAVIOUR ..... 38
2.14.5 BEHAVIOUR OF MIVOICE 5300 IP PHONES ..... 38
2.15 CONFIGURING MIVOICE 5300 IP PHONES FOR SIGNAL AND VOICE ENCRYPTION ..... 39
2.16 FACTORY CONFIGURATION OF MIVOICE 5300 IP PHONES ..... 39
2.16.1 FROM THE TERMINAL ..... 39
2.16.2 FROM THE WEB INTERFACE: ..... 40
2.17 CONFIGURATION REQUIRED IN THE SYSTEM ..... 40
2.17.1 DECLARING MIVOICE 5300 IP PHONES IN THE SYSTEM ..... 40
2.17.2 CONFIGURING THE ENCODING LAWS ASSOCIATED WITH THE TERMINALS MIVOICE 5300 IP PHONE ..... 40

2.18 CONFIGURING THE ETHERNET SWITCH ..... 41
2.19 QOS ON THE IP NETWORK ..... 41
2.20 TROUBLESHOOTING SOLUTIONS ..... 42
2.20.1 STATUS OF THE LATEST TERMINAL FIRMWARE DOWNLOADING ..... 42
2.20.2 STATUS OF THE LATEST TERMINAL CONFIGURATION FILE DOWNLOADING ..... 43
2.20.3 THE TERMINAL IS LOCKED AND IS NO LONGER ACCESSIBLE VIA THE LAN. ..... 43
2.20.4 PRESS THE TERMINAL KEYS DOES NOT HAVE ANY EFFECT ..... 44
2.20.5 THE CONFIGURATION FILE SETTINGS ARE NOT TAKEN INTO ACCOUNT ..... 44
2.20.6 THE CONFIGURATION FILES ARE NOT DOWNLOADED. ..... 44
2.21 INFORMATION MESSAGES ON THE MIVOICE 5300 IP PHONE SCREEN ..... 45
2.21.1 DOWNLOAD FAILURE ..... 45
2.21.2 NET SETTINGS CHANGED, REBOOT NECESSARY ..... 45
2.21.3 SW UPDATE REQUIRED, UPDATING ..... 45

**3 MITEL 6000 SIP PHONES ..... 47**

3.1 MITEL 6730 SIP PHONES ..... 48
3.1.1 DESCRIPTION OF MITEL 6730 SIP PHONE ..... 48
3.1.2 SALES CODE FOR MITEL 6730 SIP PHONE ..... 48
3.2 MITEL 6731 SIP PHONES ..... 48
3.2.1 DESCRIPTION OF MITEL 6731 SIP PHONE ..... 49
3.2.2 SALES CODE FOR MITEL 6731 SIP PHONE ..... 49
3.3 MITEL 6735 SIP PHONES ..... 49
3.3.1 DESCRIPTION OF MITEL 6735 SIP PHONE ..... 49
3.3.2 SALES CODE FOR MITEL 6735 SIP PHONE ..... 49
3.4 MITEL 6737 SIP PHONES ..... 49
3.4.1 DESCRIPTION OF MITEL 6737 SIP PHONE ..... 49
3.4.2 SALES CODE FOR MITEL 6737 SIP PHONE ..... 50
3.5 MITEL 6739 SIP PHONES ..... 50
3.5.1 DESCRIPTION OF MITEL 6739 SIP PHONE ..... 50
3.5.2 SALES CODE FOR MITEL 6739 SIP PHONE ..... 50
3.6 MITEL 6751 SIP PHONES ..... 50
3.6.1 DESCRIPTION OF MITEL 6751 SIP PHONE ..... 50
3.6.2 SALES CODE FOR MITEL 6751 SIP PHONE ..... 50
3.7 MITEL 6753 SIP PHONES ..... 51
3.7.1 DESCRIPTION OF MITEL 6753 SIP PHONE ..... 51
3.7.2 SALES CODE FOR MITEL 6753 SIP PHONE ..... 51
3.8 MITEL 6755 SIP PHONES ..... 51
3.8.1 DESCRIPTION OF MITEL 6755 SIP PHONE ..... 51
3.8.2 SALES CODE FOR MITEL 6755 SIP PHONE ..... 51
3.9 MITEL 6757 SIP PHONES ..... 52
3.9.1 DESCRIPTION OF MITEL 6757 SIP PHONE ..... 52
3.9.2 SALES CODE FOR MITEL 6757 SIP PHONE ..... 52
3.10 MITEL 6863 SIP PHONES ..... 52
3.10.1 DESCRIPTION OF MITEL 6863 SIP PHONE ..... 52
3.10.2 SALES CODE FOR MITEL 6863 SIP PHONE ..... 52
3.11 MITEL 6865 SIP PHONES ..... 53
3.11.1 DESCRIPTION OF MITEL 6865 SIP PHONE ..... 53
3.11.2 SALES CODE FOR MITEL 6865 SIP PHONE ..... 53
3.12 MITEL 6867 SIP PHONES ..... 53
3.12.1 DESCRIPTION OF MITEL 6867 SIP PHONE ..... 53
3.12.2 SALES CODE FOR MITEL 6867 SIP PHONE ..... 53
3.13 MITEL 6869 SIP PHONES ..... 54
3.13.1 DESCRIPTION OF MITEL 6869 SIP PHONE ..... 54
3.13.2 SALES CODE FOR MITEL 6869 SIP PHONE ..... 54
3.14 MITEL 6873 SIP PHONES ..... 54
3.14.1 DESCRIPTION OF MITEL 6873 SIP PHONE ..... 54
3.14.2 SALES CODE FOR MITEL 6873 SIP PHONE ..... 54
3.15 POSTE MIVOICE 6920 IP PHONE ..... 55
3.15.1 DESCRIPTION OF MIVOICE 6920 IP PHONE ..... 55

3.15.2 SALES CODE FOR MIVOICE 6920 IP PHONE ..... 55
3.16 POSTE MIVOICE 6930 IP PHONE ..... 55
3.16.1 DESCRIPTION OF MIVOICE 6930 IP PHONE ..... 55
3.16.2 SALES CODE FOR MIVOICE 6930 IP PHONE ..... 55
3.17 POSTE MIVOICE 6940 IP PHONE ..... 56
3.17.1 DESCRIPTION OF MIVOICE 6940 IP PHONE ..... 56
3.17.2 SALES CODE FOR MIVOICE 6940 IP PHONE ..... 56
3.18 CONNECTING MITEL 6731 SIP PHONE, 6735 SIP, 6737I, 6751 SIP, 6753 SIP, 6755 SIP AND 6757 SIP 57
3.18.1 HEADSET SOCKET WIRING OF TERMINALS MITEL 6000 SIP PHONES ..... 58
3.19 CONNECTING MITEL 6730 SIP PHONE ..... 58
3.20 CONNECTING MITEL 6863 SIP PHONE ..... 59
3.21 CONNECTING MITEL 6865 SIP PHONE ..... 60
3.22 CONNECTING MITEL 6867 SIP PHONE / 6869 SIP PHONES ..... 61
3.23 CONNECTING MITEL 6873 SIP PHONES ..... 62
3.24 CONNECTING MIVOICE 6920 IP PHONES ..... 63
3.25 CONNECTING MIVOICE 6930 IP PHONES ..... 64
3.26 CONNECTING MIVOICE 6940 IP PHONES ..... 65
3.27 EXPANSION MODULES ..... 66
3.27.1 EXPANSION MODULE M670I ..... 67
3.27.2 EXPANSION MODULE M675I ..... 67
3.27.3 EXTENSION MODULE M680I ..... 68
3.27.4 EXTENSION MODULE M685I ..... 68
3.27.5 EXTENSION MODULE M695 ..... 69
3.28 DETACHABLE MAGNETIC KEYPAD K680I ..... 70
3.29 OPTIONAL ACCESSORIES ..... 71
3.30 TELEPHONY FEATURES OF MITEL 6000 SIP PHONES ..... 72
3.31 MIVOICE 5000 ARCHITECTURES WITH MIVOICE 6000 SIP PHONES ..... 73
3.32 MITEL 6000 SIP PHONE CONFIGURATION MODES ..... 74
3.32.1 CONNECTING THE DATA SWITCH ..... 75
3.33 CONFIGURING MITEL 6000 SIP PHONE FOR THE DUAL HOMING FUNCTION ..... 76
3.34 CONFIGURING MITEL 6000 SIP PHONE FOR THE MD5 AUTHENTICATION FUNCTION ..... 77
3.34.1 WORKING PRINCIPLE: ..... 77
3.34.2 CONFIGURING THE MD5 PASSWORD IN THE IPBX ..... 77
3.34.3 CONFIGURING THE MD5 PASSWORD MANUALLY IN THE MITEL 6000 SIP PHONES ..... 78
3.34.4 AUTOMATIC CONFIGURATION OF THE MD5 PASSWORD IN THE MITEL 6000 SIP PHONES 78
3.35 CONFIGURING MITEL 6000 SIP PHONES IN THE 802.1X ENVIRONMENT ..... 80
3.35.1 WORKING PRINCIPLE: ..... 80
3.35.2 CONFIGURING THE 802.1X AUTHENTICATION SETTINGS OF MITEL 6000 SIP PHONES ... 81
3.35.3 MITEL 6000 SIP PHONE AUTHENTICATION PROCEDURES ..... 81
3.35.4 SWITCH BEHAVIOUR ..... 82
3.35.5 BEHAVIOUR OF MITEL 6000 SIP PHONES ..... 82
3.36 CONFIGURING MITEL 6000 SIP PHONES FOR SIGNAL AND VOICE ENCRYPTION ..... 83
3.37 CONFIGURING MITEL 6000 SIP PHONES FOR THE MULTI-LINE AND MULTI-CCOS FUNCTION .83
3.38 CONFIGURING MITEL 6000 SIP PHONES FOR THE BLF FUNCTION ..... 83
3.38.1 WORKING PRINCIPLE: ..... 83
3.38.2 PROGRAMMING THE BLF FUNCTION FOR A MITEL 6000 SIP PHONE ..... 83
3.39 RESTORING THE FACTORY SETTINGS OF MITEL 6000 SIP PHONES ..... 85
3.39.1 FROM THE TERMINAL ..... 85
3.39.2 FROM THE WEB INTERFACE ..... 85
3.40 NTP SERVER ..... 86
3.41 CONFIGURATION REQUIRED IN THE SYSTEM ..... 87
3.41.1 DECLARING MITEL 6000 SIP PHONES IN THE SYSTEM ..... 87
3.41.2 CONFIGURING THE ENCODING LAWS ASSOCIATED WITH MITEL TERMINALS MITEL 6000 SIP PHONES ..... 87
3.42 CONFIGURING THE ETHERNET SWITCH ..... 88
3.43 QOS ON THE IP NETWORK ..... 88

3.44 TROUBLESHOOTING SOLUTIONS ..... 89
3.44.1 WHY DOES MY MITEL 6000 SIP PHONE DISPLAY "APPLICATION MISSING"? ..... 89
3.44.2 WHY DOES MY MITEL 6000 SIP PHONE DISPLAY "NO SERVICE"? ..... 89
3.44.3 WHY DOESN'T MY MITEL 6000 SIP PHONE RECEIVE THE FTP SERVER IP ADDRESS FROM THE DHCP SERVER? ..... 90

**4 DESCRIPTION OF MIVOICE 5361 DIGITAL PHONE, 5370 DIGITAL PHONE AND 5380 DIGITAL PHONE 91**

4.1 MIVOICE 5361 DIGITAL PHONE ..... 91
4.1.1 DESCRIPTION OF MIVOICE 5361 DIGITAL PHONE ..... 91
4.1.2 SALES CODE FOR MIVOICE 5361 DIGITAL PHONE ..... 91
4.2 MIVOICE 5370 DIGITAL PHONE ..... 92
4.2.1 DESCRIPTION OF MIVOICE 5370 DIGITAL PHONE ..... 92
4.2.2 SALES CODE FOR MIVOICE 5370 DIGITAL PHONE ..... 92
4.3 MIVOICE 5380 DIGITAL PHONE ..... 92
4.3.1 DESCRIPTION OF MIVOICE 5380 DIGITAL PHONE ..... 92
4.3.2 SALES CODE FOR MIVOICE 5380 DIGITAL PHONE ..... 92
4.4 MIVOICE 5300 DIGITAL PHONE CONNECTIONS ..... 93
4.4.1 HEADSETS COMPATIBLE WITH MIVOICE 5370 DIGITAL PHONE AND 5380 IP PHONE .. 93
4.5 MIVOICE M530 EXTENSION MODULE ..... 94
4.5.1 CHARACTERISTICS OF THE MIVOICE M530 EXTENSION MODULE ..... 94
4.6 OPTIONAL ACCESSORIES ..... 94
4.7 MANAGEMENT OF MIVOICE 5361 DIGITAL PHONE, 5370 DIGITAL PHONE AND 5380 DIGITAL PHONE BY TMA ..... 95

**5 TMA - GENERAL INFORMATION (MIVOICE 5000 MANAGER AND INTEGRATED SYSTEM) ..... 97**

5.1 GENERAL INFORMATION ..... 97
5.2 MAIN DIFFERENCES BETWEEN TMA ON MIVOICE 5000 MANAGER AND INTEGRATED TMA .... 99
5.2.1 DIFFERENCES IN TERMS OF DESIGN ..... 99
5.2.2 FUNCTIONAL DIFFERENCES ..... 99
5.2.3 MENUS AVAILABLE ACCORDING TO TERMINAL RANGE ..... 99
5.2.4 COMPARISON OF THE TMA SERVICES AVAILABLE IN MIVOICE 5000 MANAGER AND INTEGRATED INTO MIVOICE 5000 ..... 100

**6 MANAGING TERMINALS WITH THE TMA INTEGRATED INTO MIVOICE 5000 ..... 101**

6.1 PRESENTATION AND PRINCIPLES ..... 101
6.2 LAUNCHING THE TMA APPLICATION ..... 102
6.3 CONFIGURING TMA ..... 103
6.3.1 CONFIGURING THE TERMINALS ..... 103
6.3.2 ENCRYPTING CONFIGURATION FILES ..... 103
6.4 MODEL MANAGEMENT ..... 104
6.5 FTP SERVER CONFIGURATION PARAMETERS ..... 104
6.5.1 INTRODUCTION ..... 104
6.5.2 USING THE FTP SERVER INTEGRATED INTO MITEL 5000 GATEWAYS AND MIVOICE 5000 SERVER. ..... 105
6.6 DHCP SERVER CONFIGURATION PARAMETERS ..... 108
6.6.1 INTRODUCTION ..... 108
6.6.2 STARTING THE INTEGRATED DHCP SERVICE ON MITEL 5000 GATEWAYS ..... 108
6.6.3 STARTING THE INTEGRATED DHCP SERVICE ON MIVOICE 5000 SERVER ..... 108
6.7 DEPLOYING THE TERMINALS FOR A NEW MITEL 5000 GATEWAYS INSTALLATION ..... 109
6.7.1 PRINCIPLE ..... 109
6.7.2 CONFIGURING THE SYSTEM VIA CTRL I ..... 109
6.7.3 CONFIGURING NETWORK PARAMETERS IN MITEL 5000 GATEWAYS ..... 110
6.7.4 CONFIGURING FLOW SEPARATION IN MITEL 5000 GATEWAYS ..... 111
6.7.5 CONFIGURING THE INTEGRATED SERVICES IN MITEL 5000 GATEWAYS WHILE STARTING THE SYSTEM ..... 111
6.7.6 DEFINING THE PARAMETERS FOR AUTOMATIC DEPLOYMENT OF MITEL 6000 SIP PHONES IN MITEL 5000 GATEWAYS ..... 112
6.7.7 DEFINING THE PARAMETERS OF THE INTEGRATED DHCP SERVER

IN MITEL 5000 GATEWAYS ..... 113
6.7.8 RESTARTING MITEL 5000 GATEWAYS ..... 114
6.7.9 CHECKING THE CONFIGURATION OF THE INTEGRATED DHCP SERVER ON MITEL 5000 GATEWAYS: ..... 115
6.7.10 CHECKING THE CONFIGURATION OF THE INTEGRATED FTP SERVER IN MITEL 5000 GATEWAYS ..... 115
6.7.11 CHECKING THE CONFIGURATION OF THE PRODUCTION SOFTWARE RELEASE OF MIVOICE 5300 IP PHONES AND MITEL 6000 SIP PHONES ..... 115
6.8 DEPLOYING MITEL 6000 SIP PHONES ON A NEW MITEL 5000 GATEWAYS INSTALLATION ..... 116
6.8.1 DEPLOYING MITEL 6000 SIP PHONES THROUGH MANUAL LOGIN ..... 117
6.8.2 DEPLOYING MITEL 6000 SIP PHONES VIA MIVOICE 5000 USER PORTAL ..... 118
6.8.3 DEPLOYING MITEL 6000 SIP PHONES AUTOMATICALLY ..... 119
6.8.4 DEPLOYING MITEL 6000 SIP PHONES THROUGH AN EXCEL FORM ..... 120
6.8.5 MULTI-COMPANY CONFIGURATION ..... 124
6.8.6 INVENTORY OF MITEL 6000 SIP PHONES ..... 124
6.9 DEPLOYING MIVOICE 5300 IP PHONES ON A NEW MITEL 5000 GATEWAYS INSTALLATION ..... 126
6.9.1 DEPLOYING MIVOICE 5300 IP PHONES AUTOMATICALLY THROUGH MANUAL LOGIN ..... 126
6.9.2 DEPLOYING MIVOICE 5300 IP PHONES THROUGH AN EXCEL FORM ..... 128
6.9.3 INVENTORY OF MIVOICE 5300 IP PHONES ..... 131
6.10 DEPLOYING TERMINALS ON A NEW MIVOICE 5000 SERVER INSTALLATION ..... 133
6.10.1 PRINCIPLE ..... 133
6.10.2 CONFIGURING THE SYSTEM VIA CTRL I ..... 133
6.10.3 CONFIGURING FLOW SEPARATION IN MIVOICE 5000 SERVER ..... 134
6.10.4 INSTALLING THE INTEGRATED SERVICES ON MIVOICE 5000 SERVER ..... 134
6.10.5 AUTOMATIC START OF THE INTEGRATED SERVICES ON MIVOICE 5000 SERVER ..... 135
6.10.6 DEFINING THE PARAMETERS FOR AUTOMATIC DEPLOYMENT OF MITEL 6000 SIP PHONES IN MIVOICE 5000 SERVER ..... 135
6.10.7 AUTOMATIC CONFIGURATION OF THE INTEGRATED DHCP SERVER PARAMETERS ON MIVOICE 5000 SERVER ..... 136
6.10.8 RESTARTING MIVOICE 5000 SERVER ..... 137
6.10.9 CHECKING THE CONFIGURATION OF THE INTEGRATED DHCP SERVER ON MIVOICE 5000 SERVER ..... 138
6.10.10 CHECKING THE CONFIGURATION OF THE INTEGRATED FTP SERVER ON MIVOICE 5000 SERVER ..... 138
6.11 DEPLOYING MITEL 6000 SIP PHONES ON A NEW MIVOICE 5000 SERVER INSTALLATION ..... 139
6.12 INVENTORY OF MITEL 6000 SIP PHONES ..... 140
6.13 DEPLOYING MIVOICE 5300 IP PHONES ON A NEW MIVOICE 5000 SERVER INSTALLATION ..... 140
6.14 INVENTORY OF MIVOICE 5300 IP PHONES ..... 140
6.15 UPDATING MITEL 6000 SIP PHONES MANUALLY ..... 141
6.15.1 PRINCIPLE ..... 141
6.15.2 GLOBAL DATA UPDATE ..... 143
6.15.3 SPECIFIC DATA UPDATE ..... 146
6.15.4 UPDATING MITEL 6000 SIP PHONE SOFTWARE RELEASE ..... 151
6.15.5 DISTRIBUTING THE NEW PRODUCTION RELEASE PARAMETERS ..... 153
6.15.6 MANAGING THE LIST OF TERMINALS FOR MITEL 6000 SIP PHONES ..... 154
6.16 TEST MODE FOR MITEL 6000 SIP PHONES ..... 156
6.16.1 UPDATING MITEL 6000 SIP PHONE SOFTWARE RELEASE IN TEST MODE ..... 156
6.16.2 DISTRIBUTING THE NEW TEST SOFTWARE RELEASE PARAMETERS ..... 158
6.16.3 UPDATING THE GLOBAL DATA OF TERMINALS IN THE TEST SOFTWARE RELEASE ..... 158
6.16.4 UPDATING THE SPECIFIC DATA OF INDIVIDUAL TERMINALS USED WITH THE TEST SOFTWARE ..... 160
6.16.5 EXITING THE TEST MODE ..... 162
6.17 UPDATING MIVOICE 5300 IP PHONES MANUALLY ..... 164
6.17.1 PRINCIPLE ..... 164
6.17.2 GLOBAL DATA UPDATE ..... 166
6.17.3 SPECIFIC DATA UPDATE ..... 167
6.17.4 UPDATING MIVOICE 5300 IP PHONE SOFTWARE RELEASE ..... 168
6.17.5 DISTRIBUTING THE PARAMETERS OF THE NEW PRODUCTION RELEASE ..... 169

6.17.6 MANAGING THE LIST OF TERMINALS FOR MIVOICE 5300 IP PHONES ..... 170
6.18 TEST MODE FOR MIVOICE 5300 IP PHONES ..... 171
6.18.1 UPDATING MIVOICE 5300 IP PHONE SOFTWARE RELEASE IN TEST MODE ..... 171
6.18.2 DISTRIBUTING THE NEW TEST SOFTWARE RELEASE PARAMETERS ..... 173
6.18.3 UPDATING THE GLOBAL DATA OF THE TERMINALS USED WITH THE TEST SOFTWARE 173
6.18.4 UPDATING THE SPECIFIC DATA OF TERMINALS USED WITH THE TEST SOFTWARE 173
6.18.5 CHECKING THAT THE UPDATE PROCESS IS WORKING CORRECTLY FOR SPECIFIC DATA IN TEST MODE ..... 173
6.18.6 EXITING THE TEST MODE ..... 173
6.19 MANAGING MIVOICE 5300 DIGITAL PHONES (TDM) ..... 176
6.19.1 INVENTORY OF MIVOICE 5300 DIGITAL PHONES ..... 176
6.19.2 MANAGING THE LIST OF TERMINALS FOR MIVOICE 5300 DIGITAL PHONES ..... 177
6.19.3 UPDATING THE TERMINAL SOFTWARE RELEASE OF MIVOICE 5300 DIGITAL PHONES .. 179
6.19.4 CHECKING THAT THE UPDATE PROCESS IS WORKING CORRECTLY FOR THE PRODUCTION SOFTWARE RELEASE ..... 179
6.20 TEST MODE FOR MIVOICE 5300 DIGITAL PHONES ..... 181
6.20.1 UPDATING MIVOICE 5300 DIGITAL PHONE SOFTWARE RELEASE IN TEST MODE ..... 181
6.20.2 STARTING THE UPDATE OF THE NEW TEST VERSION ..... 181
6.20.3 CHECKING THAT THE TEST SOFTWARE RELEASE UPDATE IS WORKING CORRECTLY . 183
6.20.4 EXITING THE TEST MODE ..... 183
6.21 ADDITIONAL TMA FUNCTIONS ..... 185
6.21.1 DOWNLOADING FILES INDIVIDUALLY ..... 185
6.21.2 EXPORTING THE DATA CONTAINED IN THE MITEL 6000 SIP PHONE AND MIVOICE 5300 IP PHONE CONFIGURATION FILES ..... 186
6.21.3 EXPORTING THE DATA CONTAINED IN THE INVENTORIES OF MITEL 6000 SIP PHONE, MIVOICE 5300 IP PHONE AND MIVOICE 5300 DIGITAL PHONE ..... 186
6.21.4 PRINTING OUT THE DATA CONTAINED IN THE INVENTORIES OF MITEL 6000 SIP PHONE, MIVOICE 5300 IP PHONE AND MIVOICE 5300 DIGITAL PHONE ..... 187
6.21.5 EVENTS LOG ..... 187
6.21.6 DELETING A SOFTWARE RELEASE ..... 188
6.22 PROGRAMMING SYSTEM KEYS FOR MITEL 6000 SIP PHONES (TEMPLATE MANAGEMENT) . 189
6.23 DEPLOYING AND CONFIGURING NEW MITEL 6000 SIP PHONES IN A WORKING INSTALLATION. 190
6.23.1 DEPLOYING NEW MITEL 6000 SIP PHONES AUTOMATICALLY ..... 190
6.23.2 CHECKING THE DEPLOYMENT OF MITEL 6000 SIP PHONES ..... 190
6.23.3 DAY-TO-DAY MANAGEMENT OF THESE NEW MITEL 6000 SIP PHONES ..... 190
6.24 DEPLOYING AND CONFIGURING NEW MIVOICE 5300 IP PHONES IN A WORKING INSTALLATION 191
6.24.1 DEPLOYING NEW MIVOICE 5300 IP PHONES AUTOMATICALLY ..... 191
6.24.2 CHECKING THE DEPLOYMENT OF MIVOICE 5300 IP PHONES ..... 191
6.24.3 DAY-TO-DAY MANAGEMENT OF THESE NEW MIVOICE 5300 IP PHONES ..... 191
6.25 AUTOMATICALLY DEPLOYING AND UPDATING MIVOICE 5300 IP PHONE AND MITEL 6000 SIP PHONES WHILE UPGRADING A MIVOICE 5000 SYSTEM ..... 192
6.25.1 PRINCIPLE ..... 192
6.25.2 UPGRADING A MIVOICE 5000 SYSTEM ..... 192
6.25.3 AUTOMATIC UPDATE OF MITEL 6000 SIP PHONES AND MIVOICE 5300 IP PHONES ... 193
6.25.4 DEPLOYING NEW MIVOICE 5300 IP PHONES AUTOMATICALLY ..... 193
6.25.5 DEPLOYING NEW MITEL 6000 SIP PHONES AUTOMATICALLY ..... 193
6.25.6 CHECKING THE DEPLOYMENT OF MIVOICE 5300 IP PHONES AND MITEL 6000 SIP PHONES ..... 193
6.26 UPDATING MIVOICE 5300 DIGITAL PHONE SOFTWARE RELEASE WHILE UPGRADING A MIVOICE 5000 SYSTEM ..... 194
6.26.1 UPDATING MIVOICE DIGITAL PHONES VIA THE INTEGRATED TMA ..... 194
6.26.2 STARTING THE UPDATE OF THE NEW PRODUCTION RELEASE ..... 194
6.26.3 CHECKING THE MIVOICE 5300 DIGITAL PHONE UPDATE ..... 194

**7 MANAGING TERMINALS WITH TMA HOSTED BY MIVOICE 5000 MANAGER ..... 195**

7.1 PRESENTATION AND PRINCIPLES ..... 195
7.2 LAUNCHING THE TMA ..... 195
7.3 CONFIGURING THE TMA APPLICATION ..... 197
7.3.1 ACTIVATING AND DEACTIVATING TMA-EP MODE ..... 197
7.3.2 CONFIGURING THE TERMINALS ..... 197
7.3.3 ENCRYPTING CONFIGURATION FILES ..... 197
7.3.4 ENABLING AND DISABLING REMOTE WORKER MANAGEMENT ..... 197
7.3.5 EXCLUDING ONE OR MORE SITES ..... 197
7.3.6 TESTING THE CONFIGURATION ..... 198
7.4 MODEL MANAGEMENT ..... 198
7.5 DEPLOY THE TERMINALS ..... 199
7.5.1 PRINCIPLE ..... 199
7.6 DEPLOYING MITEL 6000 SIP PHONES ..... 200
7.6.1 DEPLOYING MITEL 6000 SIP PHONES THROUGH MANUAL LOGIN ..... 200
7.6.2 DEPLOYING MITEL 6000 SIP PHONES VIA MIVOICE 5000 USER PORTAL ..... 201
7.6.3 DEPLOYING MITEL 6000 SIP PHONES AUTOMATICALLY ..... 201
7.6.4 DEPLOYING MITEL 6000 SIP PHONES THROUGH AN EXCEL FORM ..... 201
7.6.5 DEFINING THE PRODUCTION TERMINAL SOFTWARE PACKAGE ..... 206
7.6.6 DEFINING THE PARAMETERS OF THE SOFTWARE PACKAGE USED WITH THE PRODUCTION RELEASE ..... 206
7.7 DEPLOYING MIVOICE 5300 IP PHONES ..... 208
7.7.1 DEPLOYING MIVOICE 5300 IP PHONES AUTOMATICALLY VIA THE MANUAL LOGIN FUNCTION ..... 208
7.7.2 DEPLOYING MIVOICE 5300 IP PHONES THROUGH AN EXCEL FORM ..... 208
7.8 UPDATING MITEL 6000 SIP PHONES MANUALLY ..... 213
7.8.1 PRINCIPLE ..... 213
7.8.2 GLOBAL DATA UPDATE ..... 213
7.8.3 SPECIFIC DATA UPDATE ..... 213
7.8.4 UPDATING MITEL 6000 SIP PHONE SOFTWARE RELEASE ..... 214
7.8.5 DISTRIBUTING THE PARAMETERS OF THE NEW PRODUCTION RELEASE ..... 214
7.8.6 MANAGING THE LIST OF TERMINALS FOR MITEL 6000 SIP PHONES ..... 215
7.9 TEST MODE FOR MITEL 6000 SIP PHONES ..... 217
7.9.1 UPDATING MITEL 6000 SIP PHONE SOFTWARE RELEASE IN TEST MODE ..... 217
7.9.2 DISTRIBUTING THE NEW TEST SOFTWARE RELEASE PARAMETERS ..... 217
7.9.3 UPDATING THE GLOBAL DATA OF THE TERMINALS USED WITH THE TEST SOFTWARE . 217
7.9.4 UPDATING THE SPECIFIC DATA OF TERMINALS USED WITH THE TEST SOFTWARE . 217
7.9.5 EXITING THE TEST MODE ..... 219
7.10 UPDATING MIVOICE 5300 IP PHONES MANUALLY ..... 220
7.10.1 PRINCIPLE ..... 220
7.10.2 GLOBAL DATA UPDATE ..... 220
7.10.3 SPECIFIC DATA UPDATE ..... 220
7.10.4 UPDATING MIVOICE 5300 IP PHONE SOFTWARE RELEASE ..... 220
7.10.5 DISTRIBUTING THE PARAMETERS OF THE NEW PRODUCTION RELEASE ..... 221
7.10.6 MANAGING THE LIST OF TERMINALS FOR MIVOICE 5300 IP PHONES ..... 222
7.11 TEST MODE FOR MIVOICE 5300 IP PHONES ..... 223
7.11.1 UPDATING MIVOICE 5300 IP PHONE SOFTWARE RELEASE IN TEST MODE ..... 223
7.11.2 DISTRIBUTING THE NEW TEST SOFTWARE RELEASE PARAMETERS ..... 224
7.11.3 MIVOICE 5300 IP PHONE GLOBAL DATA UPDATE IN THE TEST SOFTWARE RELEASE ..... 224
7.11.4 UPDATING THE SPECIFIC DATA OF MIVOICE 5300 IP PHONES IN THE TEST SOFTWARE RELEASE ..... 225
7.11.5 EXITING THE TEST MODE ..... 226
7.12 MANAGING MIVOICE 5300 DIGITAL PHONES (TDM) ..... 227
7.12.1 INVENTORY OF MIVOICE 5300 DIGITAL PHONES ..... 227
7.12.2 MANAGING THE LIST OF TERMINALS FOR MIVOICE 5300 DIGITAL PHONES ..... 228

7.12.3 UPDATING THE SOFTWARE RELEASE OF MIVOICE 5300 DIGITAL PHONES ..... 229
7.12.4 CHECKING THAT THE UPDATE PROCESS IS WORKING CORRECTLY FOR THE PRODUCTION SOFTWARE RELEASE ..... 231
7.13 TEST MODE FOR MIVOICE 5300 DIGITAL PHONES ..... 232
7.13.1 UPDATING MIVOICE 5300 DIGITAL PHONE SOFTWARE RELEASE IN TEST MODE ..... 232
7.13.2 DEFINING THE NEW TEST VERSION ..... 232
7.13.3 STARTING THE UPDATE OF THE NEW TEST VERSION ..... 232
7.13.4 CHECKING THAT THE UPDATE PROCESS IS WORKING CORRECTLY FOR THE TEST SOFTWARE RELEASE ..... 234
7.13.5 EXITING THE TEST MODE ..... 234
7.14 MANAGING VIRTUAL TDM MIVOICE 5300 DIGITAL PHONES ..... 236
7.14.1 INVENTORY OF MIVOICE 5300 DIGITAL PHONES ..... 236
7.14.2 UPDATING THE SOFTWARE RELEASE OF MIVOICE 5300 DIGITAL PHONES ..... 236
7.15 ADDITIONAL TMA FUNCTIONS ..... 237
7.15.1 DOWNLOADING FILES INDIVIDUALLY ..... 237
7.15.2 EXPORTING THE DATA CONTAINED IN THE CONFIGURATION FILES OF MITEL 6000 SIP PHONES AND MIVOICE 5300 IP PHONES ..... 237
7.15.3 EXPORTING THE DATA CONTAINED IN INVENTORIES OF MITEL 6000 SIP PHONE, MIVOICE 5300 IP PHONE AND MIVOICE 5300 DIGITAL PHONE ..... 238
7.15.4 PRINTING THE DATA CONTAINED IN INVENTORIES OF MITEL 6000 SIP PHONE, MIVOICE 5300 IP PHONE AND MIVOICE 5300 DIGITAL PHONE ..... 238
7.15.5 EVENT LOG ..... 238
7.15.6 DELETING A SOFTWARE RELEASE ..... 239
7.15.7 IPBX CONFIGURATION ..... 240
7.16 PROGRAMMING THE SYSTEM KEYS FOR MITEL 6000 SIP PHONES (TEMPLATE MANAGEMENT) ..... 241
7.17 TROUBLESHOOTING SOLUTIONS ..... 241
7.17.1 INVENTORY IS NOT UPDATED AUTOMATICALLY ..... 241

**8 MANAGING A HETEROGENEOUS NETWORK WITH TMA HOSTED BY MIVOICE 5000 MANAGER ..... 243**

**9 CONFIGURING THE DHCP SERVER INTEGRATED MIVOICE 5000 SYSTEMS ..... 245**

9.1 DHCP SERVICE HOME PAGE ..... 246
9.2 CREATING A NEW DHCP CONFIGURATION ..... 246
9.3 CONFIGURING THE GENERAL PARAMETERS OF THE DHCP SERVER ..... 246
9.4 CONFIGURING THE STANDARD PARAMETERS OF THE SUBNET ..... 249
9.5 DEFINING THE SPECIFIC SUBNET PARAMETERS FOR MIVOICE 5300 IP PHONES ..... 250
9.6 DEFINING THE SPECIFIC SUBNET PARAMETERS FOR MITEL 6000 SIP PHONE AND 8000I ... 252
9.7 DEFINING THE SPECIFIC SUBNET PARAMETERS FOR TERMINALS I7XX ..... 254
9.8 DEFINING THE SPECIFIC SUBNET PARAMETERS FOR THE DECT/IP BASE STATIONS (RFPS) .... 256
9.9 DEFINING THE SPECIFIC SUBNET PARAMETERS FOR MITEL DECT/SIP BASE STATIONS (RFPS) 258
9.10 DEFINING THE SPECIFIC SUBNET PARAMETERS FOR TERMINALS 312I ..... 260
9.11 DEFINING THE SPECIFIC SUBNET PARAMETERS FOR TERMINALS TA7102I ..... 262
9.12 DEFINING THE SPECIFIC SUBNET PARAMETERS FOR TERMINALS 6900 IP PHONES,UC360 AND 5304 PHONE ..... 263
9.13 INCORPORATING TERMINALS 6900, UC360 AND 5304 IN THE INTEGRATED DHCP OF MIVOICE 5000 ..... 264
9.13.1 INTRODUCTION ..... 264
9.13.2 DESCRIPTION OF DHCP ..... 264
9.13.3 AUTOMATIC UPGRADE ..... 266
9.13.4 RESULT ..... 267
9.14 "6XXXI/ALL_MODELS OR SPECIFIC MODEL" AND "MIVOICE CONFERENCE UNIT" SELECTED 269
9.14.1 DESCRIPTION ..... 269
9.14.2 PROCEDURE ..... 269
9.15 "6XXXI/ALL_MODELS OR SPECIFIC MODEL" AND "UC360_5304" SELECTED ..... 272
9.15.1 DESCRIPTION ..... 272

9.15.2 PROCDURE....272
9.16 CONFIGURING THE PARAMETERS OF A SUBNET HOST....275
9.17 CONFIGURING THE PARAMETERS OF A SUBNET EXCLUSION....276
9.18 TEMPLATES MANAGEMENT....277
9.18.1 ADDING A NEW TEMPLATE....277
9.18.2 DELETING AN EXISTING TEMPLATE....278
9.19 GENERATING THE CONFIGURATION FILE USED BY THE INTEGRATED DHCP SERVER....280
9.20 MODIFYING THE PARAMETERS OF A DHCP CONFIGURATION....281
9.21 RESTORING AND DELETING AN ARCHIVE....282
9.22 VIEWING THE DHCP SERVER CONFIGURATION....283
9.23 DHCP SERVICE STATUS:....283
9.24 VIEW DHCP LEASES....283
9.25 CONFIGURATION WITH TWO SUBNETS IN SHARED NETWORK MODE.....283
9.26 MANAGING INTEGRATED DHCP SERVER DATA WHILE BACKING UP DATA FROM MIVOICE 5000 284
9.27 MANAGING THE INTEGRATED DHCP SERVER DATA WHILE UPGRADING MIVOICE 5000....284
9.28 REDUNDANT INTEGRATED DHCP SERVER ON A REDUNDANT MIVOICE 5000 SERVER....285

**10 CONFIGURING AN EXTERNAL DHCP SERVER....287**

10.1 CONFIGURING THE EXTERNAL DHCP SERVER FOR MITEL 6000 SIP PHONES....287
10.1.1 STANDARD DHCP SETTINGS OR OPTIONS MANAGED BY MITEL 6000 SIP PHONES....287
10.1.2 SPECIFIC DHCP SETTINGS MANAGED BY MITEL 6000 SIP PHONES VIA OPTION 43...288
10.1.3 CONFIGURING A DHCP SERVER ON A WINDOWS 2000/2003 PLATFORM FOR MITEL 6000 SIP PHONES....289
10.1.4 CONFIGURING A DHCP SERVER ON A MIVOICE 5000 SERVER PLATFORM FOR MITEL 6000 SIP PHONES....299
10.2 CONFIGURING THE EXTERNAL DHCP SERVER FOR MIVOICE 5300 IP PHONES....305
10.2.1 STANDARD DHCP SETTINGS OR OPTIONS MANAGED BY MIVOICE 5300 IP PHONE,..305
10.2.2 SPECIFIC DHCP SETTINGS MANAGED BY MIVOICE 5300 IP PHONES VIA OPTION 43 306
10.2.3 CONFIGURING A DHCP SERVER ON A PLATFORM WINDOWS 2000/2003....307
10.2.4 CONFIGURING A DHCP SERVER ON A MIVOICE 5000 SERVER PLATFORM FOR MIVOICE 5300 IP PHONES....312
10.3 CONFIGURING THE EXTERNAL DHCP SERVICE IN A REDUNDANT MIVOICE 5000 SERVER CONFIGURATION....314

**11 CONFIGURING THE FTP SERVERS USED BY TMA....315**

11.1 CONFIGURING AN FTP SERVER ON A PLATFORM WINDOWS 2000/2003 FOR MIVOICE 5300 IP PHONES....315
11.1.1 ACCOUNTS ASSOCIATED WITH THE STORAGE DIRECTORIES FOR MIVOICE 5300 IP PHONES....315
11.1.2 CREATING THE ACCOUNT USED BY TERMINALS FOR THE PRODUCTION VERSION .316
11.1.3 CREATING THE ACCOUNT USED BY TERMINALS FOR THE TEST VERSION....316
11.1.4 CREATING THE ACCOUNT USED BY TMA (PRODUCTION VERSION)....317
11.1.5 CREATING THE ACCOUNT USED BY TMA (TEST VERSION)....317
11.2 CONFIGURING AN FTP SERVER ON A MIVOICE 5000 SERVER PLATFORM FOR MIVOICE 5300 IP PHONES....318
11.2.1 ACCOUNTS ASSOCIATED WITH THE STORAGE DIRECTORIES FOR MIVOICE 5300 IP PHONES....318
11.2.2 CREATING THE ACCOUNT USED BY TERMINALS FOR THE PRODUCTION VERSION .319
11.2.3 CREATING THE ACCOUNT USED BY TERMINALS FOR THE TEST VERSION....319
11.2.4 CREATING THE ACCOUNT USED BY TMA (PRODUCTION VERSION)....320
11.2.5 CREATING THE ACCOUNT USED BY TMA (TEST VERSION)....320
11.2.6 CREATING THE MNGT_FTP_53XXIP GROUP....320
11.2.7 CREATING THE MNGT_TEST_53XXIP GROUP....321
11.2.8 CHANGE THE OWNER AND GROUP ASSOCIATED WITH THE MIVOICE 5300 IP PHONE. .. 321
11.2.9 MODIFY THE RIGHTS ASSOCIATED WITH THE MIVOICE 5300 IP PHONE DIRETORY. .321

11.2.10 CHANGE THE OWNER AND GROUP ASSOCIATED WITH THE TEST DIRECTORY..... 321
11.2.11 CHANGE THE RIGHTS ASSOCIATED WITH THE TEST DIRECTORY..... 321
11.2.12 MODIFY THE FILE VSFTPD.CONF UNDER /ETC/VSFTPD. ..... 322
11.3 CONFIGURING AN FTP SERVER ON A PLATFORM WINDOWS 2000/2003 FOR MITEL 6000 SIP PHONES..... 325
11.3.1 ACCOUNTS ASSOCIATED WITH THE STORAGE DIRECTORIES FOR MITEL 6000 SIP PHONES ..... 325
11.3.2 CREATING THE ACCOUNT USED BY TERMINALS TO DEPLOY THE PRODUCTION VERSION..... 326
11.3.3 CREATING THE ACCOUNT USED BY TERMINALS FOR THE PRODUCTION VERSION. 326
11.3.4 CREATING THE ACCOUNT USED BY TERMINALS FOR THE TEST VERSION..... 327
11.3.5 CREATING THE ACCOUNT USED BY TMA (PRODUCTION VERSION)..... 327
11.3.6 CREATING THE ACCOUNT USED BY TMA (TEST VERSION)..... 328
11.4 CONFIGURING AN FTP SERVER ON A PLATFORM MIVOICE 5000 SERVER FOR MITEL 6000 SIP PHONES..... 329
11.4.1 ACCOUNTS ASSOCIATED WITH THE STORAGE DIRECTORIES FOR MITEL 6000 SIP PHONES ..... 329
11.4.2 CREATING THE ACCOUNT USED TO DEPLOY THE PRODUCTION VERSION ON MITEL 6000 SIP PHONES ..... 330
11.4.3 CREATING THE ACCOUNT USED BY TERMINALS FOR THE PRODUCTION VERSION. 330
11.4.4 CREATING THE ACCOUNT USED BY TERMINALS FOR THE TEST VERSION..... 331
11.4.5 CREATING THE ACCOUNT USED BY TMA (PRODUCTION VERSION)..... 331
11.4.6 CREATING THE ACCOUNT USED BY TMA (TEST VERSION)..... 332
11.4.7 CREATING THE MNGT_FTP_67XXI GROUP ..... 332
11.4.8 CREATING THE MNGT_TEST_67XXI GROUP ..... 332
11.4.9 CHANGE THE OWNER AND GROUP ASSOCIATED WITH THE MITEL 6700 SIP PHONE DIRECTORY. ..... 333
11.4.10 MODIFY THE RIGHTS ASSOCIATED WITH THE MITEL 6700 SIP PHONE DIRECTORY. 333
11.4.11 CHANGE THE OWNER AND GROUP ASSOCIATED WITH THE TEST FOLDER. ..... 333
11.4.12 CHANGE THE RIGHTS ASSOCIATED WITH THE TEST DIRECTORY..... 333
11.4.13 MODIFY THE FILE VSFTPD.CONF UNDER /ETC/VSFTPD. ..... 333

**12 APPENDIX 1..... 335**

12.1 INSTALLING DHCP PACKAGING IN LINUX REDHAT 5 ..... 335

**13 APPENDIX 2..... 337**

13.1 LIST AND MEANING OF THE STANDARD NETWORK PARAMETERS USED BY THE DHCP SERVER INTEGRATED INTO MITEL 5000 GATEWAYS AND MIVOICE 5000 SERVER ..... 337

**14 APPENDIX 3..... 339**

14.1 EXAMPLES OF ARCHITECTURES ASSOCIATED WITH THE DHCP SERVER INTEGRATED INTO MITEL 5000 GATEWAYS..... 339
14.2 THE DEVICES ARE INSTALLED ON DIFFERENT SUBNETS AND THE CLIENT ALREADY HAS A DHCP SERVER:..... 339
14.2.1 ONLY ONE DHCP SERVER. ALL THE NETWORK DEVICES, INCLUDING THE INTEGRATED DHCP SERVER, ARE INSTALLED ON THE SAME IP NETWORK: ..... 341

**15 APPENDIX 4: MANAGING THE TERMINALS MANUALLY MIVOICE 5300 IP PHONE AND MITEL 6000 SIP PHONE ..... 343**

15.1 CONFIGURING AN FTP SERVER ON A PLATFORM WINDOWS 2000/2003 FOR MIVOICE 5300 IP PHONES..... 343
15.2 CONFIGURING AN FTP SERVER ON A PLATFORM MIVOICE 5000 SERVER FOR MIVOICE 5300 IP PHONES..... 344
15.3 CONFIGURING AN FTP SERVER ON A WINDOWS 2000/2003 PLATFORM FOR MITEL 6000 SIP PHONES..... 347
15.4 CONFIGURING AN FTP SERVER ON A MIVOICE 5000 SERVER PLATFORM FOR MITEL 6000 SIP PHONES..... 347

**16 APPENDIX 5: CONFIGURING MIVOICE 5300 IP PHONES MANUALLY ..... 351**

16.1 DEFAULT CONFIGURATION WHEN THE TERMINAL IS INSTALLED FOR THE FIRST TIME ..... 351
16.2 MANUAL CONFIGURATION FROM MIVOICE 5300 IP PHONES ..... 352
16.3 MANUAL CONFIGURATION FROM THE WEB INTERFACE ..... 360
16.3.1 MODES SUPPORTED BY THE TERMINAL'S INTEGRATED SWITCH PORTS ..... 362
16.4 DOWNLOADING THE FIRMWARE AND CONFIGURATION FILES OF MIVOICE 5300 IP PHONES ..... 364
16.4.1 MIVOICE 5300 IP PHONE DOWNLOADING TOOLS ..... 364
16.4.2 MIVOICE 5300 IP PHONE PARAMETER PRIORITY ..... 365
16.4.3 CONFIGURATION FILE FORMAT OF MIVOICE 5300 IP PHONES ..... 366

**17 APPENDIX 6: MANUAL CONFIGURATION OF MITEL 6000 SIP PHONES ..... 369**

17.1 DEFAULT CONFIGURATION WHEN THE TERMINAL IS INSTALLED FOR THE FIRST TIME ..... 369
17.2 MANUAL CONFIGURATION FROM MITEL 6000 SIP PHONES ..... 369
17.2.1 CONFIGURE THE NETWORK SETTINGS OF MITEL 6000 SIP PHONES ..... 370
17.2.2 CONFIGURING THE FTP SERVER PARAMETERS OF MITEL 6000 SIP PHONES ..... 370
17.2.3 CONFIGURE THE SIP SETTINGS OF MITEL 6000 SIP PHONES. ..... 370
17.2.4 DEFINE THE LAN PORT VLAN PARAMETERS OF MITEL 6000 SIP PHONES ..... 371
17.2.5 DEFINE THE PC PORT VLAN PARAMETERS OF MITEL 6000 SIP PHONES ..... 372
17.2.6 RESTART THE MITEL 6000 SIP PHONES ..... 372
17.2.7 CONFIGURE MITEL 6000 SIP PHONES IN FRENCH LANGUAGE: ..... 372
17.3 MANUAL CONFIGURATION OF MITEL 6000 SIP PHONES VIA THE WEB INTERFACE ..... 373
17.3.1 CONFIGURING THE BASIC NETWORK SETTINGS OF MITEL 6000 SIP PHONES ..... 373
17.3.2 CONFIGURING THE FTP SERVER FOR MITEL 6000 SIP PHONES ..... 373
17.3.3 CONFIGURING THE SIP SETTINGS OF MITEL 6000 SIP PHONES ..... 374
17.3.4 RESTART THE MITEL 6000 SIP PHONES ..... 374
17.3.5 CONFIGURING THE WEB INTERFACE LANGUAGE ..... 374
17.3.6 DOWNLOADING A LANGUAGE PACK ON MITEL 6000 SIP PHONES ..... 375
17.4 CONFIGURING ETHERNET SWITCHES FOR MITEL 6000 SIP PHONES ..... 376
17.4.1 REMOTE SUPPLY TO MITEL 6000 SIP PHONES ..... 376
17.4.2 MODES SUPPORTED BY THE TERMINAL'S INTEGRATED SWITCH PORTS ..... 376
17.5 DOWNLOADING THE FIRMWARE AND CONFIGURATION FILES OF MITEL 6000 SIP PHONES ..... 377
17.5.1 MITEL 6000 SIP PHONE DOWNLOADING TOOLS ..... 377
17.5.2 MITEL 6000 SIP PHONE PARAMETER PRIORITY ..... 378
17.5.3 MITEL 6000 SIP PHONE SPECIFIC CONFIGURATION FILE FORMAT ..... 378

# LIST OF TABLES

*TABLEAU 11.1 : .....315*
*TABLEAU 11.2 : .....318*
*TABLEAU 11.3 : .....325*
*TABLEAU 11.4 : .....329*

# 1 ABOUT THIS DOCUMENT

## 1.1 PURPOSE OF THIS DOCUMENT

This document describes, for MiVoice 5000 R6.5, the tools used to install, deploy, configure and manage on site, in simple or complex network configurations, MiVoice 5300 IP Phones/MiVoice 5300 Digital Phones and Mitel6000 SIP Phones, as well as the available options associated with these terminals.

## 1.2 TARGET AUDIENCE OF THIS DOCUMENT

This document is intended for installers, and provides the following information:

- List of MiVoice 5300 IP Phones, references, options and main features,
- List of Mitel 6000 SIP Phones, references, options and main features,
- List of MiVoice 5300 Digital Phones, references, options and main features,
- Manual deployment of MiVoice 5300 IP Phones and Mitel 6000 SIP Phones in a simplified network architecture using the inbuilt FTP server on Mitel 5000 Gateways,
- Automatic deployment of MiVoice 5300 IP Phones and Mitel 6000 SIP Phones in a simplified network architecture using the inbuilt FTP and DHCP server on Mitel 5000 Gateways,
- Automatic deployment of MiVoice 5300 IP Phone and Mitel 6000 SIP Phone in a complex network architecture with a DHCP server on a Windows 2000/2003 or LINUX (RedHat Enterprise) platform and an external FTP server on a Windows 2000/2003 or LINUX (RedHat Enterprise) platform.
- Automatic deployment of MiVoice 5300 IP Phone, with the use of the TMA hosted by MiVoice 5000 Manager in a complex configuration comprising one or more multi-sites, or one or more external DHCP servers and one or more external FTP servers.
- Download of the Mivoice 5300 Digital Phones via TMA

## 1.3 SCOPE OF THIS DOCUMENT

This manual applies to proprietary MiVoice 5300 IP Phones (5360 IP, 5361 IP, 5370 IP, 5380 IP Phone IP), proprietary MiVoice 5300 Digital Phones (5361 Digital, 5370 Digital, 5380 Digital) and to Mitel 6000 SIP Phones (6730 SIP, 6731 SIP, 6735 SIP, 6737 SIP, 6739 SIP, 6753 SIP, 6755 SIP, 6757 SIP, 6863 SIP, 6865 SIP, 6867 SIP, 6869 SIP, 6873 SIP, 6920 IP, 6930 IP and 6940 IP) within the perimeter of MiVoice 5000 R6.5.

# 1.4 TERMINOLOGY

## 1.4.1 TERMS AND EXPRESSIONS

**SIP terminal** IP terminal using SIP (Session Initiation Protocol).

**Mitel 5000 Gateways** This term refers to all XS, XL and XD iPBXs.

**MiVoice 5000 or MiVoice 5000 Server**

Telephone switching system installed on a PC running with Linux Redhat or CentOs

**XS, XL, XD** MiVoice 5000 series physical gateways.

**LLDP** (Link Layer Discovery Protocol, IEEE 802.1AB) is a type of frame that allows network equipment
(station, switch, router, IP phone) to communicate their identity and their functions to their environment.

**aastra.cfg** This file contains the parameters to apply to Mitel 6000 SIP Phone (the terminals' global configuration file).

<**MAC>.cfg** Configuration file specific to a terminal: @MAC.cfg (example: 00085D3A2451.cfg).

**Mitel Web UI** This is the interface provided by the terminal via a browser, which allows most of the terminal parameters to be defined.

**Deployment server**

We distinguish between two types of FTP servers: those used in the deployment phase and those used for day-to-day management. The terminals obtain the deployment server address through DHCP the first time it is deployed. When the terminal is registered with its PBX, it is channelled back to the day-to-day management servers.

**IP phone UI** This is the interface on the terminal itself, accessible through interactive menus.

**SIP password** Password used by the terminal to meet an MD5 challenge of the PBX.

**User password** 4-digit password for each PBX subscription.

**Login site** The login site is the first site to which the terminal tries to register after receiving its address via DHCP or configuration file. The terminal will then be channelled back to the site on which it is declared (reference site).

**Main site** The main site is the site on which the subscription is declared. This term is used in particular when the subscription is backed up on a backup site.

**Backup site** The backup site of a subscription is the site to which the subscription characteristics of the main site is copied.

**Reference site** The reference site is the main site on which the subscription is declared. If the main site and backup site are both active, the reference site is the main site. If the main site becomes inactive, the reference site becomes the backup site.

### 1.4.2 ABBREVIATIONS

| | |
|---|---|
| **AASP:** | **A**amadeus **S**timulus **P**rotocol |
| **CD-ROM:** | **C**ompact **D**isk-**R**ead **O**nly **M**emory |
| **DCF:** | **C**onfiguration **I**nstructions |
| **DHCP:** | **D**ynamic **H**ost **C**onnection **P**rotocol |
| **FTP:** | **F**ile **T**ransfer **P**rotocol |
| **GSI:** | **G**ateway **S**IP **I**nterface |
| **IPS:** | **IP S**erver |
| **IRQ:** | **I**nterrupt **R**e**Q**uest |
| **LAN:** | **L**ocal **A**rea **N**etwork |
| **LCD:** | **L**iquid **C**rystal **D**isplay |
| **LED:** | **L**ight **E**mitting **D**iode |
| **LLDP:** | **L**ink **L**ayer **D**iscovery **P**rotocol |
| **HF:** | **H**ands **F**ree |
| **NTP:** | **N**etwork **T**ime **P**rotocol |
| **OS:** | **O**perating **S**ystem |
| **PBX:** | **P**rivate **B**ranch e**X**change |
| **PC:** | **P**ersonal **C**omputer |
| **RAM:** | **R**andom **A**ccess **M**emory |
| **RST** | **R**eset |
| **MMC:** | **M**an **M**achine **C**ommand |
| **SIP:** | **S**ession **I**nitiation **P**rotocol |
| **TFTP:** | **T**rivial **F**ile **T**ransfer **P**rotocol |
| **VLAN:** | **V**irtual **L**ocal **A**rea **N**etwork |

# 1.5 REFERENCE DOCUMENTS

## 1.5.1 TERMINAL RELATED DOCUMENTS

**Note : Documentation is no longer provided with the offer. It is available on the distributor's Extranet – column: Marketing and Sales.**

**Note : The terminal documentation can be consulted on the distributor's extranet, in the column SERVICES / MiVoice 5000 / Knowledge base / Terminals.**

| PRODUCT | DOCUMENT NAME | REFERENCE |
|---|---|---|
| 6730 SIP/6731 SIP | User Guide | AMT/PUD/TR/0077/EN |
| 6739 SIP | User Guide | AMT/PUD/TR/0078/EN |
| 6753 SIP | User Guide | AMT/PUD/TR/0076/EN |
| 6755 SIP / 6735 SIP | User Guide | AMT/PUD/TR/0069/EN |
| 6757 SIP / 6737 SIP | User Guide | AMT/PUD/TR/0075/EN |
| 6863 SIP | User Guide | AMT/PUD/TR/0143/EN |
| 6865 SIP | User Guide | AMT/PUD/TR/0144/EN |
| 6867 SIP | User Guide | AMT/PUD/TR/0145/EN |
| 6869 SIP | User Guide | AMT/PUD/TR/0147/EN |
| 6873 SIP | User Guide | AMT/PUD/TR/0148/EN |
| 6920 SIP | User Guide | AMT/PUD/TR/0149/EN |
| 6930 SIP | User Guide | AMT/PUD/TR/0150/EN |
| 6940 SIP | User Guide | AMT/PUD/TR/0151/EN |
| 5380 Digital, 5380 IP Phone IP | User Guide | AMT/PUD/TR/0015/EN |
| 5370 Digital, 5370 IP | User Guide | AMT/PUD/TR/0016/EN |
| 5361 Digital, 5361 IP | User Guide | AMT/PUD/TR/0106/EN |
| 5360 IP | User Guide | AMT/PUD/TR/0042/EN |

### 1.5.2 SYSTEM RELATED DOCUMENTS

| SYSTEM | DOCUMENT NAME | REFERENCE |
|---|---|---|
| Mitel 5000 Gateways and MiVoice 5000 Server | Multi-site management | AMT/PTD/PBX/0081/EN |
| Mitel 5000 Gateways | Functional description and Hard-ware installation | AMT/PTD/PBX/0150/EN |
| MiVoice 5000 Server and Mitel 5000 Gateways | Activation | AMT/PTD/PBX/0151/EN |
| MiVoice 5000 Server and Mitel 5000 Gateways | Operating manual | AMT/PTD/PBX/0080/EN |
| MiVoice 5000 Server | Installation and Configuration Guide for Redundant MiVoice 5000 Server | AMT/PTD/PBX/0083/EN |
| MiVoice 5000 Manager | User guide | AMT/PUD/NMA/0003/EN |
| Mitel 5000 Gateways, MiVoice 5000 Server and MiVoice 5000 manger | Updating by repository | AMT/PTD/PBX/0155/2/ For R6.5, minimum edition 2 |

# 2 MIVOICE 5300 IP PHONES

The MiVoice 5300 series IP Phone consists of four terminal types:

- MiVoice 5360 IP Phone,
- MiVoice 5361 IP Phone
- MiVoice 5370 IP Phone,
- MiVoice 5380 IP Phone.

MiVoice 5370 IP Phone and 5380 IP Phone can be used with an extension module.

The proprietary MiVoice 5360 IP, 5370 IP and 5380 IP Phones are managed as of release R5000.1 R5.1A on Mitel 5000 Gateways and MiVoice 5000 Server.

The proprietary MiVoice 5361 IP Phone is managed as of release MiVoice 5000 R5.3 on Mitel 5000 Gateways and MiVoice 5000 Server.

**MiVoice 5300 IP Phone replacement protocol**

The protocol used is a proprietary AASP protocol transmitted via the UDP/SIP layer. Signalling is integrated in the body of the SIP message.

The terminal's behaviour is determined by the system (ergonomics, audio, etc.).

**ATTENTION : MiVoice 5300-series IP Phones are also compatible with the ASCOTEL range. They have the same sales references.**

## 2.1 MIVOICE 5360 IP PHONES




### 2.1.1 DESCRIPTION OF MIVOICE 5360 IP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 2.1.2 SALES CODE FOR MIVOICE 5360 IP PHONE

The sales code for MiVoice 5360 IP Phone without mains unit is 20350774.

## 2.2 MIVOICE 5361 IP PHONES




### 2.2.1 DESCRIPTION OF MIVOICE 5361 IP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 2.2.2 SALES CODE FOR MIVOICE 5361 IP PHONE

The sales code for MiVoice 5361 IP Phone without mains unit is 20351331.

## 2.3 MIVOICE 5370 IP PHONES



### 2.3.1 DESCRIPTION OF MIVOICE 5370 IP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 2.3.2 SALES CODE FOR MIVOICE 5370 IP PHONE

The sales code for MiVoice 5370 IP Phone without mains unit is 20350775.

## 2.4 MIVOICE 5380 IP PHONES



### 2.4.1 DESCRIPTION OF MIVOICE 5380 IP PHONE

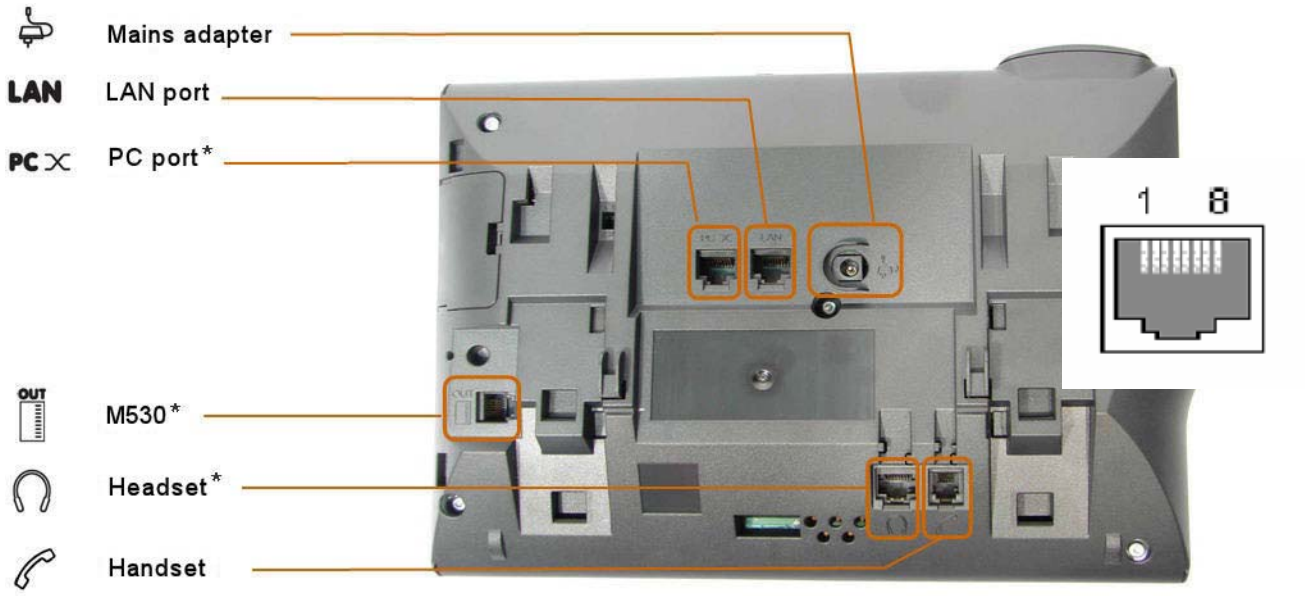
A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 2.4.2 SALES CODE FOR MIVOICE 5380 IP PHONE

The sales code for MiVoice 5380 IP Phone with AZERTY keypad and without mains unit is 20350788.

The sales code for MiVoice 5380 IP Phone with QWERTY keypad and without mains unit is 20350776.

## 2.5 MIVOICE 5300 IP PHONE CONNECTIONS

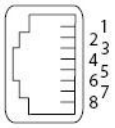



* Only on terminals MiVoice 5370 IP Phone and MiVoice 5380 IP Phone

**Note: The Ethernet port labelled "PC" does not supply power online via other network devices.**

**Note: The mains adapter and PoE (via the local area network) can be connected simultaneously and thus allow redundancy.**

### 2.5.1 REMOTE POWER SUPPLY TO MIVOICE 5300 IP PHONES (POE)

| RJ45 socket | Pin | Signal | Remote power supply variant 1 | Remote power supply variant 2 |
|---|---|---|---|---|
|  | 1 | Rx | DC+ | — |
| | 2 | Rx | DC+ | — |
| | 3 | Tx | DC- | — |
| | 4 | — | — | DC+ |
| | 5 | — | — | DC+ |
| | 6 | Tx | DC- | — |
| | 7 | — | — | DC- |
| | 8 | — | — | DC- |



The Ethernet ports of a PoE can support a nominal voltage of 48V DC either on the pairs of data (1-2, 3-6) or on the free pairs (4-5, 7-8), but not both at the same time. In the absence of automatic power supply, an optional mains adapter is available, but it requires a mains socket (see “Optional accessories”, page 28).

## 2.5.2 HEADSETS COMPATIBLE WITH MIVOICE 5370 DIGITAL PHONE AND 5380 IP PHONE

The headset socket for 5370 and 5380 IP Phones is compatible with DHSG standard.

The wiring for the RJ45 headset is as follows:

| Pin | Description |
|---|---|
| 1 | Signalling (from headset to terminal) |
| 2 | 0V (Signal GND) |
| 3 | MIC- |
| 4 | Loudspeaker |
| 5 | Loudspeaker |
| 6 | MIC+ |
| 7 | DC in (3.3 V DC) |
| 8 | Signalling (from terminal to headset) |

Input impedance (MIC-/MIC+): 15 k ohms

Output impedance (loudspeaker/loudspeaker):150 ohms

The following headsets have Mitel price references:

- GN2000 from GN-Netcom: wired headset with sales code AHR0204AA01
- GN9120 from GN-Netcom: wireless headset with sales code AHR0207AA01
- GN9350 from GN-Netcom: wireless headset with DHSG cable and sales code AHR0207AA01

Headsets GN9120 and GN9350 have two operating modes:

- DHSG mode,
- RHL mode.

**ATTENTION : The "automatic off-hook" function offered by the DHSG protocol is only available on MiVoice 5300 IP Phone and MiVoice 5300 Digital Phone.**

Since 5370 IP and 5380 IP Phones are DHSG compatible, remote line seizure / on-hook is via the headset button or by lifting / placing the headset on its base.

RHL mode allows these headsets to be used on other Mitel phones (6755/6757, M/i740, M/i760, 6753 SIP, 6755 SIP, 6757 SIP, 6730 SIP, 6731 SIP, 6739 SIP, 6865 SIP, 6867 SIP, 6869 SIP)

A special cable is obligatory for headsets GN9350 and GN9120 to work in DHSG mode. It comes with headset GN9350.

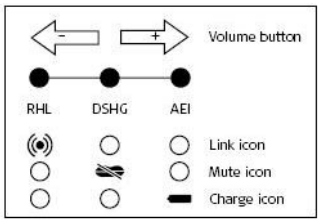


To configure the operating mode of headset GN9120, proceed as follows:

- Place the headset on the base with the "online" LED facing you
- Press simultaneously the "+" and "-" volume buttons on the headset for 6 seconds (headset always on the base) until the "online" LED blinks rapidly.

You are then in interface change mode and can set GN 9120 to RHL or DHSG mode.

- To select the required mode, use the "+" volume button to move to the right, and the "-" volume button to move to the left. The three indicator lights of the base indicate the mode to which GN9120 is set; see illustration below.




If you fail to press the "+" volume button or "-" volume button after more than 15 seconds, the last mode selected will be activated.

- To exit the interface changing mode, press the "+" volume and "-" volume button simultaneously for 6 seconds.

To configure the operating mode of headset GN9350, proceed as follows:

- Using the arrows ◀ ▶ , go to RHL Interface menu on the base display.
- Select any of the 4 interfaces from the menu using the arrows ◀ ▶ .
- Press OK to confirm the interface.

## 2.6 ELECTRICAL POWER CONSUMPTION OF MIVOICE 5300 IP PHONE

The table below defines:

- The maximum power supplied by the Switch port according to PoE class,
- The minimum and maximum consumption of MiVoice 5300 IP Phone according to the negotiated PoE class and the presence of one or more MiVoice M530 extension modules (maximum one extension module for MiVoice 5370 IP Phone, and up to three extension modules for MiVoice 5380 IP Phone).

| Class | Maximum power supplied by the switch | Terminal's power consumption | Terminal model |
|---|---|---|---|
| 1 | 4.0 W | 0.44...3.84 W | MiVoice 5361 IP Phone |
| 2 | 7.0 W | 3.84...6.49 W | MiVoice 5370 IP Phone, 5380 IP Phone |
| 3 | 15.4 W | 6.49...12.95 W | |

## 2.7 MIVOICE M530 EXTENSION MODULE

An extension module is available and can be used on MiVoice 5370 IP Phone and 5380 IP Phone.

The sales code for the MiVoice M530 expansion module is 20350804.

| Touches de fonction programmable disponibles | | | |
|---|---|---|---|
| MiVoice 5370 IP Phone | | MiVoice 5380 IP Phone | |
| Terminal | 12 | Terminal | – |
| max. 1M530 | 20 | max. 3M530 | 60 |
| Total | 32 | Total | 60 |

**Note: The "Presence" key is used as an additional programmable key.**

### 2.7.1 CHARACTERISTICS OF THE MIVOICE M530 EXTENSION MODULE

- Direct power supply from the terminal (without adding any mains unit),
- 20 programmable keys, with associated LEDs (line, dial, Do not Disturb, etc.)
- Up to 3 modules per terminal:
  - Maximum one module per MiVoice 5370 IP Phone
  - Maximum three modules per MiVoice 5380 IP Phone

**Note: The firmware of the extension module is loaded during its first connection to the terminal.**

## 2.8 OPTIONAL ACCESSORIES

A mains adapter is used to power up the terminal if the LAN switch is not 802.3af compatible and cannot be used to directly power up the terminal online on its LAN port.

This adapter supplies 48V to MiVoice 5300 IP Phones. Do not use this adapter to power up other devices.



The sales code for the MiVoice 5300 IP Phone power supply unit is 20350333.

The following accessories are available:

- Batch of 10 handset cables for MiVoice 5300 Digital Phone/ MiVoice 5300 IP Phone: AHT0531A
- Batch of 10 stands for MiVoice 5300 Digital Phone/ MiVoice 5300 IP Phone:AHT0532A
- Batch of 10 M530 extension connection cables: AHT0533A
- Batch of 10 stands for M530 extension: AHT0534A

## 2.9 TELEPHONY FEATURES OF MIVOICE 5300 IP PHONE

See the product guide for this terminal range.

## 2.10 MIVOICE 5000 ARCHITECTURES WITH MIVOICE 5300 IP PHONE

MiVoice 5300 IP Phones are declared in the systems (MiVoice 5000 Server or Mitel 5000 Gateways), and connect via the SIP service integrated into the UCV card of Mitel 5000 Gateways or via the SIP service integrated into MiVoice 5000 Server.

These terminals support the login site optimisation function. This enables the phone to register with the SIP service of a site which may be different from the site on which the terminal subscription is declared.

MiVoice 5300 IP Phones are declared either on a ToIP VLAN dedicated to terminals, or they are used both on a Data VLAN and ToIP VLAN in 802.1Q if the PC is connected to the terminal.

The FTP server used for downloading on MiVoice 5300 IP Phone (firmware and configuration files) may be hosted by:

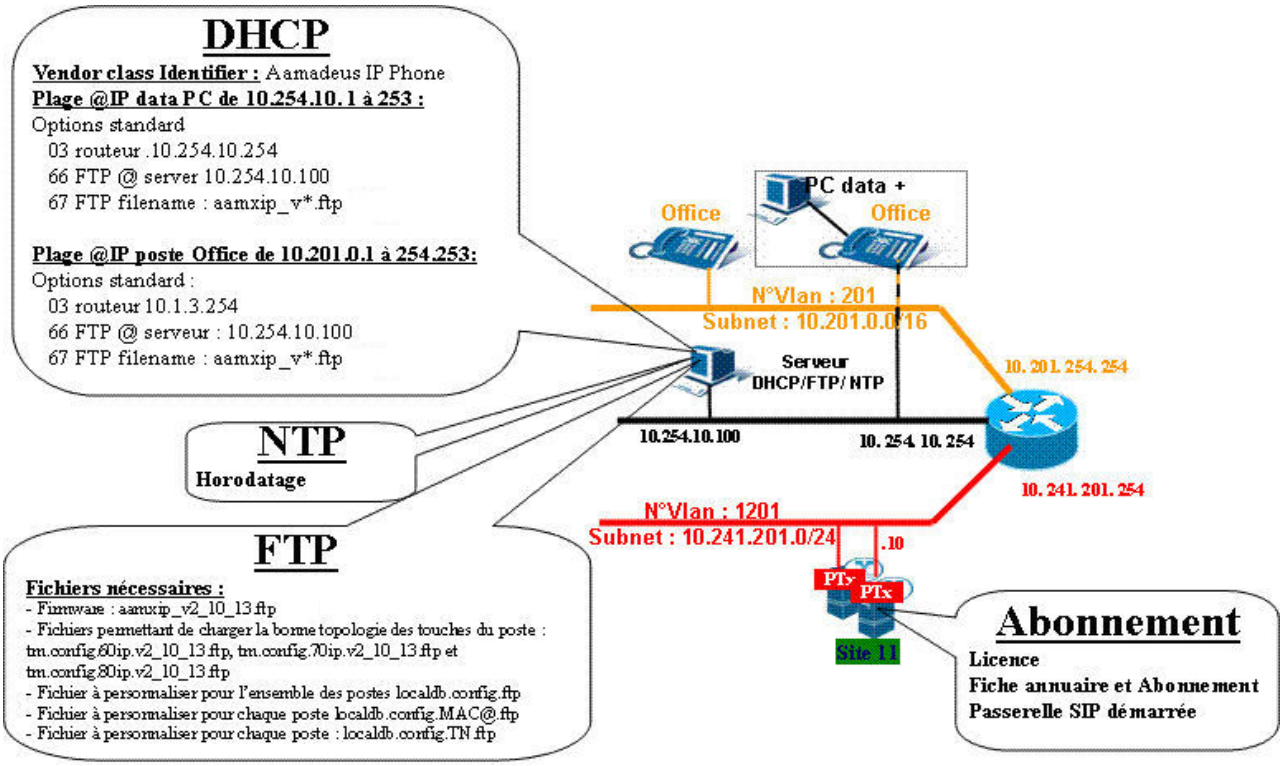
- a Windows 2000/2003 Server platform (under the network administrator's responsibility),
- a MiVoice 5000 Server (under the network administrator's responsibility),
- on Mitel 5000 Gateways. In this case, the FTP server is integrated into the UCV card, and the corresponding service will be fully managed by the system.

For each terminal, the FTP server address used must be declared:

- Either through manual configuration (directly on the terminal or via the web interface),
- Or by configuring the DHCP server.

One DHCP server, for supplying the IP address, must be accessible from the ToIP VLAN.

The 3-level Ethernet switch (router in general) handles the inter-VLAN routing, as well as DHCP relay for non-VLAN Data devices.



## 2.11 MIVOICE 5300 IP PHONE CONFIGURATION MODES

The different configuration modes of Mitel 53xxi phones are:

- For a single-site configuration, from the integrated TMA (Menu **Terminal service**) on Mitel 5000 Gateways and MiVoice 5000 Server,
- For a multi-site configuration, from the TMA installed on MiVoice 5000 Manager (Menu **Terminal service** in the **Terminal management** column),
- Manual mode through direct access in the terminal menus,
- Manual mode via the terminal management WEB interface.

**Modes recommended according to configuration:**

- **In a single-site Mitel 5000 Gateways configuration**

  Mitel recommends configuring the terminals from the integrated TMA on MiVoice 5000 also using the integrated FTP and DHCP services.

  - **During a first installation:**

    Deployment may be automatic during start in STANDARD or TOTAL mode, using CTRL + i. Refer to Section “Managing terminals with the TMA integrated into MiVoice 5000” on page 101.

  - **During iPBX update:**

    The terminals are automatically updated.

    The new iPBX software release also contains the new software releases associated with the terminals. Refer to Section .

- **In a multi-site configuration**

  In a multi-site configuration containing several sites or multi-sites, one or more external DHCP servers or one or more external FTP servers, the use of the TMA integrated into MiVoice 5000 Manager is highly recommended. This application allows software update, global and specific data update for MiVoice 5300 IP Phones, without any manual operation on the phones. Refer to Section “Managing terminals with TMA hosted by MiVoice 5000 Manager” on page 195.

- **Manual configuration of the terminals**

  To quickly deploy some terminals, direct configuration on the terminal or via the web interface may be envidsaged. Refer to Section “Appendix 5: configuring MiVoice 5300 IP phones manually” on page 351.

- **If TMA is not available**

  Be it a single-site or multi-site configuration, Mitel recommends configuring the terminals via an integrated or external DHCP server in order to automatically recover its standard network settings and manage those associated with the supplier class of MiVoice 5300 IP Phones (Aamadeus IP Phone), where necessary. The configuration is completed by downloading the software and configuration files associated with MiVoice 5300 IP Phones via an integrated or external FTP server, by manually placing these files in the appropriate storage directory.

## 2.11.1 CONNECTING THE DATA SWITCH

**MiVoice 5300 IP Phone with or without PC connection:**

In this configuration, the terminal is connected to a port that is "Terminals" and "Data" VLAN compatible: it must mark its frames in the "Terminals" VLAN. Traffic on the the Switch port is marked for the terminal and not for the PC.

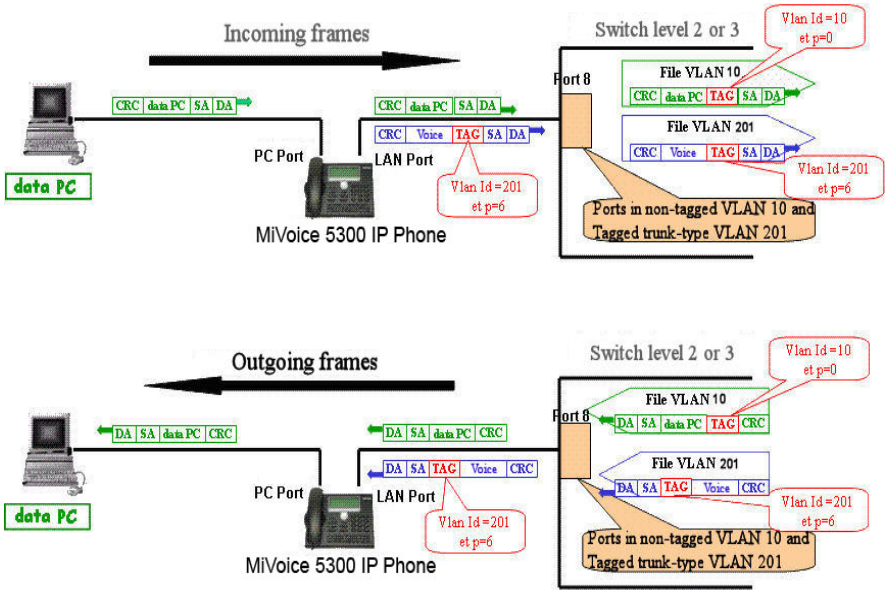
Mitel recommends configuring all the ports of the Switch to which some MiVoice 5300 IP Phones are connected in the same way, regardless of whether the terminal is standalone or connected with a PC. This way, the network administrator will not have to reconfigure the Switch ports based on PC availability or unavailability.

**Connecting the terminal:**

Connect the terminal to the switch port ("Terminals" + "Data" VLAN): the terminal will send its DHCP request on the "Data" VLAN and obtain its configuration, especially its VLAN ID, via the FTP server (firmware and configuration file) using a temporary IP address in the "Data" VLAN. The terminal will then perform a DHCP release then restart on the "Terminals" VLAN. The terminal will send a second DHCP request on the "Terminals" VLAN an obtain its full configuration.

**Example of Ethernet frame marking on the switch port:**

check that the network socket for connecting to the Data switch actually belongs to the ToIP VLAN of MiVoice 5300 IP Phones and to the Data VLAN of the PCs.



## 2.12 CONFIGURING MIVOICE 5300 IP PHONES FOR DUAL HOMING

The Dual Homing feature enables a terminal to connect to a backup site when the connection to its reference site is not possible, either because the reference site is out of service, or because its is not accessible via the network.

The diagram below gives an example of an architecture.




The settings to define on MiVoice 5300 IP Phones are:

- **PBX_ADDRESS_BACKUP** => specifies the SIP gateway IP address of the backup site
- **SIP_PORT_PBX_BACKUP** => specifies the SIP gateway listening port of the backup site

These two settings can be defined through any of the following four methods:

- Through DHCP via Option 43 (see Section)
- Via the global configuration file **localdb.config@.ftp** or specific configuration file **localdb.config.MAC@.ftp** depending on the client's network architecture (see Section 16.4.3). The information contained in the global or specific configuration file can be changed manually or via TMA.
- Manual configuration via the terminal's configuration web interface (**PBX** tab)
- Manual configuration via the terminal's sconfiguration menus (Menu **Administration** > **SIP settings** and Menu **Administration** > **PBX settings)**

*See Section 16.4.2 for the priority given to the setting if the settings are defined using several methods.*

**ATTENTION : Details about the working of the Dual Homing function and the configuration to be made on Web Admin or MiVoice 5000 Manager are given in the Multi-site Operating Manual (AMT/PTD/PBX/0083*).**

## 2.13 CONFIGURING MIVOICE 5300 IP PHONE FOR THE MD5 AUTHENTICATION FUNCTION

The MD5 password is used to authenticate the MiVoice 5300 IP Phone which connects to MiVoice 5000 Server and Mitel 5000 Gateways. This MD5 password is defined in the MiVoice 5000 Server and Mitel 5000 Gateways subscription.

This control makes it possible to prevent the registration of another device that has the same directory number by mistake or maliciously.

This function is supported by MiVoice 5300 IP Phones as of V2.12.25.

This control is made in the following cases:

- Each time the terminal is registered on the iPBX,
- Before each outgoing call.

**Note: There is no control on an incoming call.**

The MD5 password is defined once in MiVoice 5300 IP Phone and in the iPBX.

MiVoice 5300 IP Phone does not work in the following two cases:

- The MD5 password is different between MiVoice 5300 IP Phone and the iPBX.
- The MD5 password is defined in the iPBX but not in MiVoice 5300 IP Phone.

**Note: If the MD5 password is defined in MiVoice 5300 IP Phone but not in the iPBX, the terminal will be operational.**

### 2.13.1 CONFIGURING THE MD5 PASSWORD IN THE IPBX

To configure the MD5 password in the MiVoice 5000 Server and Mitel 5000 Gateways, proceed as follows:

- Go to the MD5 password definition menu:
  - this menu (124) is accessible via Subscribers / Subscriptions / Terminal authentication and MDP User Portal.
- Select the type of operation: **SIP authentication**
- Enter the First directory number.
- Enter the Last directory number.
- Select the creation mode:
  - Manual creation,
  - Automatic creation.

In case of manual creation, enter the MD5 password for the selected subscribers (alphanumeric code between 8 and 16 characters),

- Click the Confirm button to confirm the creation of MD5 password.

**Note: The Export operation is used to generate and save a file in .csv format containing the subscriptions and their MD5 password.**

**Note: Mitel OMM R2.1 type operation is used to generate and save a file in Mitel OMM R2.1 format containing the subscriptions and their MD5 passwords for DECT/IP radio fixed parts (see document AMT/PTD/PBX/0062* for the import mechanism of this file).**
**As of Mitel OMM 4.0 and R5.4, a daily or immediate data realignment mechanism from MiVoice 5000 to Mitel OMM 4.0 is used to automatically recover the MD5 password defined in the PBX for Mitel DECT/SIP radio fixed parts (Menu Subscribers > Rights > General parameters, Mitel OMM SIP management parameter application tab).**

It is possible to know whether a subscription has an already defined MD5 password.

This menu (1231) is accessible via Subscribers > Subscriptions > Characteristics: parameter **Terminal authentication** in the Characteristics tab.

### 2.13.2 CONFIGURING THE MD5 PASSWORD MANUALLY IN MIVOICE 5300 IP PHONES

This configuration method must be used in the following cases only:

- Terminal service not started in Web Admin (single-site configuration)
- TMA not configured in MiVoice 5000 Manager (multi-site configuration)

The settings to define on MiVoice 5300 IP Phones are:

- **USER_PASSWORD** => specifies the MD5 password used by MiVoice 5300 IP Phones

This parameter can be defined using any of the three methods:

- See the specific configuration file **localdb.config.MAC@.ftp** (in Section 16.4.3). In this case, the line **USER_PASSWORD** must not be in comments and contains the MD5 password. The information contained in the specific configuration file can be changed manually.
- Manual configuration via the terminal's configuration web interface (**PBX** tab, **USER_PASSWORD** field).
- Manual configuration via the terminal's configuration menus (Menu **Administration** > **User settings** > Menu **User password**

**Note: See Section 16.4.2 for the priority given to the setting if this setting is defined using several methods.**

### 2.13.3 AUTOMATIC CONFIGURATION OF THE MD5 PASSWORD IN THE MIVOICE 5300 IP PHONES

This configuration method must be used in the following cases only:

- Terminal service started in Web Admin (single-site configuration)
- TMA configured in MiVoice 5000 Manager (multi-site configuration)

Working principle:

Following the modification of the MD5 password in the iPBX (see Chapter 2.13.1), TMA is immediately notified by the management via the following two files:

- an action file,
- a modification description file containing the modified terminal and its new MD5 password.

These two files are either created by the iPBX if the terminal service is started in Web Admin, or by MiVoice 5000 Manager upon receiving an SNMP trap sent by the iPBX.

After this notification, TMA updates the specific configuration file of each terminal concerned with the right parameter and places this/these file(s) in the appropriate storage area on the FTP server (via a symbolic link, in case of integrated FTP server). At the same time, an immediate specific data update is sent to the terminal which immediately restarts to take into account its new specific configuration file containing information about the changes made to its MD5 password (deletion, modification or creation).



**ATTENTION : In this operating mode, it should be impossible to enter the MD5 parameter via the TMA MMI. Therefore, it is important to ignore this parameter (USER_PASSWORD) while distributing the parameters.**



**ATTENTION : Automatic MD5 password configuration is only available as of R5.2 SP (H2B).**

# 2.14 CONFIGURING MIVOICE 5300 IP PHONES IN THE 802.1X ENVIRONMENT

## 2.14.1 WORKING PRINCIPLE:

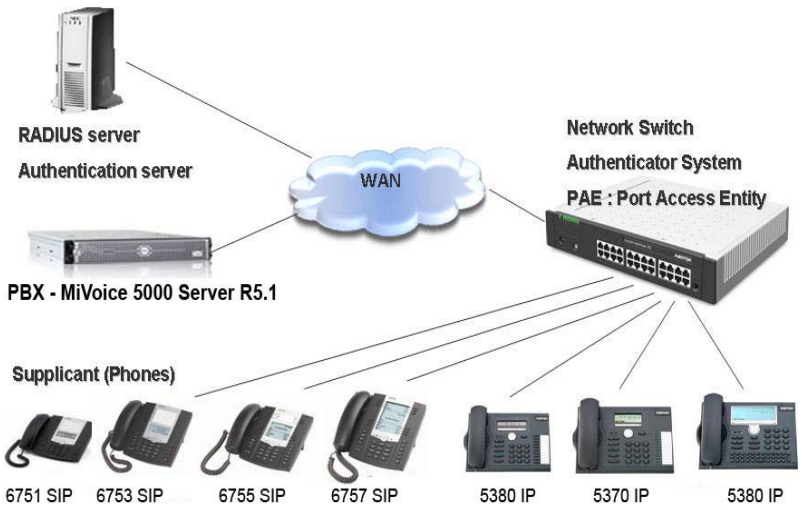
The purpose of Standard 802.1X is to authenticate to the network access during physical connection to the network. This authentication takes place before any self-configuration mechanism (for instance DHCP). In most cases, the service authorised in case of success is the Ethernet service.

The purpose of this standard is, therefore, only to validate a right to physically access the network, regardless of the transmission medium used, using some existing authentication mechanisms.

Three main players are involved in this mechanism:

- The system to authenticate (supplicant or client),
- The LAN access point (authenticator, switch, WiFi base station, etc.),
- The authentication server.

An example of 802.1X architecture is given below:




As long as he is not authenticated, the client cannot access the network; only authentication related exchanges are relayed to the authentication server via the access point. Once authenticated, the access point allows the client related traffic to flow.

The 802.1X protocol defines the use of EAP (Extensible Authentication Protocol, RFC3748), a mechanism that describes the authentication method.

MiVoice 5300 IP Phones are compatible with 802.1X authentication, in order to:

- authenticate them to a secure LAN according to the 802.1X protocol,
- allow transparent relay of the authentication request from a PC connected to the switch integrated into the terminal*

**ATTENTION : * This configuration works only on certain network devices (switche).**

### 2.14.2 CONFIGURING THE 802.1X AUTHENTICATION PARAMETERS OF MIVOICE 5300 IP PHONES

MiVoice 5300 IP Phones authenticate to the network with EAP-MD5.

Authentication is thus made using to two parameters: login and password.

The settings to define on MiVoice 5300 IP Phones are:

- X_USER => specifies the 802.1X login,
- **X_PASSWORD** => specifies the 802.1X password.

These settings can be defined through any of the following three methods:

- * Via the specific configuration file **localdb.config.MAC@.ftp** (in Section 16.4.3). In this case, the two lines above must not be in comments and contain the login and MD5 802.1X password. The information contained in the specific configuration file can be changed manually or via TMA.



**ATTENTION : * If the 802.1X authentication parameters are negotiated via the specific configuration files, the first update must be made on a network that does not implement 802.1x or on which it is deactivated.**

- Manual configuration via the terminal's configuration web interface:
  - **Network** tab, **X_USER field**
  - **Network** tab, **X_PASSWORD field**
- Manual configuration via the terminal's configuration menu:
  - Menu **Administration** > **802.1x settings**> **802.1x user**
  - Menu Administration > 802.1x settings> 802.1x password

*See Section 16.4.2 for the priority given to the settings if these settings are defined using several methods.*

### 2.14.3 MIVOICE 5300 IP PHONE AUTHENTICATION PROCEDURES

The normal authentication is procedures are as follows;

- The switch port is closed.
- MiVoice 5300 IP Phone is physically connected to the switch port.
- The switch sends an authentication request to MiVoice 5300 IP Phone then to the RADIUS server.
- The switch port is opened.
- MiVoice 5300 IP Phone connects to the LAN (ARP, DHCP, etc.).
- The terminal re-authenticates according to a configurable duration (switch setting).

### 2.14.4 SWITCH BEHAVIOUR

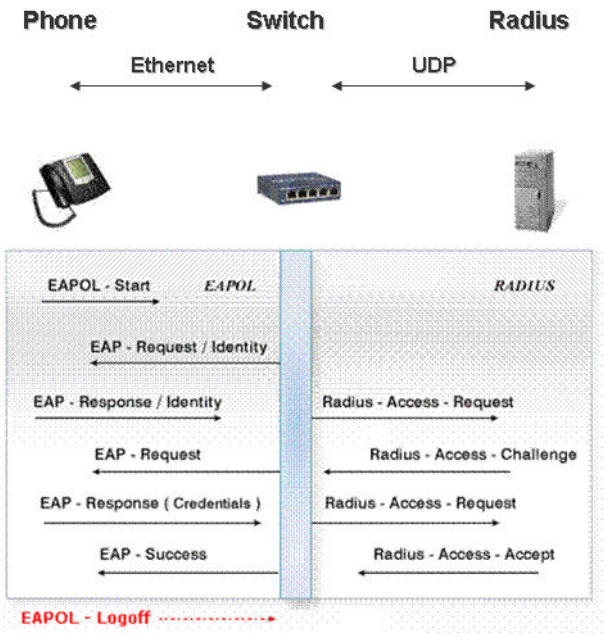
- The switch port remains closed in case of error or no response during authentication.
- A fresh authentication is started by the switch in case of error or no response to the previous authentication.
- The switch detects the terminal connection or disconnection to start authenticating the terminal.
- If the switch port is closed, new authentication attempts are made after terminal disconnection then reconnection.

### 2.14.5 BEHAVIOUR OF MIVOICE 5300 IP PHONES

The authenticator (switch) generally initiates the communication once the port becomes active and sends an EAP request frame. If the authenticator does not initiate the communication, MiVoice 5300 IP Phones can initiate it by sending an EAP start request.

MiVoice 5300 IP Phone responds to re-authentication frames (every hour). The re-authentication mechanism can be executed during the communication phase.

The exchanges are illustrated on the following diagram:



## 2.15 CONFIGURING MIVOICE 5300 IP PHONES FOR SIGNAL AND VOICE ENCRYPTION

See the call encryption operating manual (AMT/PTD/PBX/0103*).

## 2.16 FACTORY CONFIGURATION OF MIVOICE 5300 IP PHONES

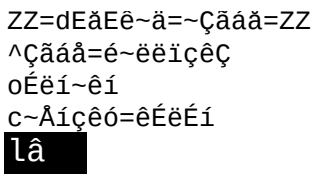
### 2.16.1 FROM THE TERMINAL

Press and hold down the **C** key for a few seconds to enter the Administration menu.

Select the **Administration** entry and press the fox key **Select.**

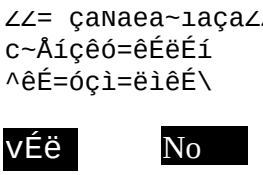
Select the **General admin** entry and press the fox key **Select.**

The screen below is displayed:



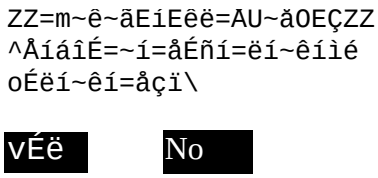

Select **Factory reset** and press the fox key **OK.**

The screen below is displayed:



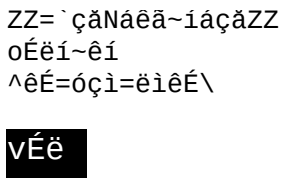

Select **Yes** to confirm the return to factory configuration.

The screen below is displayed:




Select **Yes** to confirm the return to factory configuration.

The screen below is displayed:




Press the **Yes** fox key to confirm the terminal restart.

The terminal restarts with the factory configuration.

### 2.16.2 FROM THE WEB INTERFACE:

From any tab other than the **Status** tab:

- Click the Factory Reset button then confirm the request by clicking OK.
- Wait for the request confirmation message from the terminal: "**Log: Performed factory reset**".
- Then click the **Reboot Target** button to restart the terminal with the factory settings, or cancel the modifications with the **Cancel Changes** button.

## 2.17 CONFIGURATION REQUIRED IN THE SYSTEM

### 2.17.1 DECLARING MIVOICE 5300 IP PHONES IN THE SYSTEM

Using MiVoice 5300 IP Phones requires unlocking the PROPRIETARY AUDIO licence. The type of subscription to be declared for MiVoice 5300 IP Phones is "Internal Subscriber".

Procedure:

- Go to the licence selection menu:
  - this menu (123) is accessible from System / Info / Licences.
- Enter the unlocking key corresponding to the number of MiVoice 5300 IP Phones (and/or G2KIP) deployed on the client's local area network.
- Create internal subscriber type subscriptions (LOCAL SUB).
  - This menu (121) is accessible via Subscribers / Subscriptions / Creation.

### 2.17.2 CONFIGURING THE ENCODING LAWS ASSOCIATED WITH THE TERMINALS MIVOICE 5300 IP PHONE

- Go to the encoding law selection menu:
  - this menu (441) is accessible via Network and Links / Quality of service / Voice over IP encoding law.

Select the type of call: INTERNAL

Select the type of terminal: PROPRIETARY IP

**Note: The PROPRIETARY IP terminal type corresponds to MiVoice 5300 IP Phone and i7xx.**

- Confirm by clicking the "Select item" button. In the next menu, indicate the encoding law you want according to the available bandwidth and the voice quality required.

Then check the application of the encoding laws:

- Go to the encoding law display menu:
  - this menu (442) is accessible via Network and Links / Quality of service / Display encoding laws.

## 2.18 CONFIGURING THE ETHERNET SWITCH

According to the general recommendations on the MiVoice 5300 solution, a VLAN cutting must be used:

- A VLAN comprising the PT2/IPS cards and MiVoice 5000 Servers,
- One or more VLANs containing some MiVoice 5300 IP Phones
- A VLAN containing the telephony servers (messaging, administration, etc.)
- One or more set of VLAN Data

Standalone terminals:

| TERMINAL CONFIGURATION (WEB INTERFACE/ LOCALDB.CONFIG.FTP) | CONFIGURING THE ETHERNET SWITCH |
|---|---|
| VLAN_ENABLED : OFF / VLAN_ENABLED=0 | The Ethernet switch port is in a "Terminals" VLAN without 802.1Q marking. |
| VLAN_ENABLED : ON / VLAN_ENABLED=1<br>VLAN_PRIO: 6 / VLAN_Prio=6<br>VLAN_ID : 20 / VLAN_ID=20 | The terminal and Ethernet switch mark the frames in 802.1Q on VLAN 20. |

Terminals with a PC connection:

| TERMINAL CONFIGURATION (WEB INTERFACE/ LOCALDB.CONFIG.FTP) | CONFIGURING THE ETHERNET SWITCH |
|---|---|
| VLAN_ENABLED: ON / VLAN_ENABLED=1<br>VLAN_PRIO: 6 / VLAN_PRIO=6<br>VLAN_ID: 20 / VLAN_ID=20<br><br>VLANPC_ENABLED: On / VLANPC_ENABLED=1<br>VLANPC_TAGS: Off / VLANPC_TAGS=0<br>VLANPC_PRIO: 0/ VLANPC_PRIO=0<br>VLANPC_ID: 30 / VLAN_ID=30 | The terminal and Ethernet switch mark the frames in 802.1Q on VLAN 20. The Ethernet switch and terminal PC port port are in a VLAN 30 without 802.1Q marking. |

## 2.19 QOS ON THE IP NETWORK

MiVoice 5300 IP Phones can mark the ToIP frames according to their type (signalling, RTP, RTCP) on level 2 (802.1Q) and on level 3 (DiffServ).

They can also assign a level 2 priority to traffic from the connected PC.

Level 2 devices must not modify the marking of the traffic from the terminal, unless there is an incoming traffic analysis and traffic marking.

On level 3, just activate DiffServ in the devices to take account of the ToIP frames.

The usual QoS recommendations are:

- Level 2 priority ToIP (signalling, RTP/RTCP)=6
- Level 2 priority Data=0
- Level 3 ToIP=B8h (184 decimal)
- Level 3 priority Data=00h

# 2.20 TROUBLESHOOTING SOLUTIONS

## 2.20.1 STATUS OF THE LATEST TERMINAL FIRMWARE DOWNLOADING

During each boot sequence MiVoice 5300 IP Phones send boot information associated with hitch-free firmware download (where necessary). This information is sent by the terminal in a field contained in the REGISTER and is also visible in the terminal's Web interface status tab, via the **Software download status** field.

The following information may appear in the **Software download status** field:

Normal case:

- **Idle (0000)**. This information is sent if the terminal has started and there is no need at that moment to load new firmware.

Connection to FTP server failed:

- **Unknown (0300):** Cause unknown
- **ConnectionErr (0301):** Connection error
- **LoginErr (0302):** Login incorrect
- **PathErr (0303):** Incorrect storage directory access path
- **LoginErr (0304):** File transfer error

Firmware file problem:

- **NoAamadeusArchive (0500):** It is not MiVoice 5300 IP Phone firmware
- **FileNotFound (0501):** File not found
- **FileNameNok (0502):** Incorrect file name

Problem with firmware file size:

- **Unknown (0800):** unknown file size
- **FileTooShort (0801):**
- **ImageTooBig(0802):**

Problem writing the firmware file in FLASH:

- **Unknown (0A00):** Cause unknown
- **FlashChecksumError (0A03):** Checksum error

Firmware loaded successfully:

- **UploadComplete (0B00):** Firmware loaded correctly:

### 2.20.2 STATUS OF THE LATEST TERMINAL CONFIGURATION FILE DOWNLOADING

During each boot sequence MiVoice 5300 IP Phones send boot information associated with hitch-free configuration file download. This information is sent by the terminal in a field contained in the REGISTER and is also visible in the terminal's Web interface status tab, via the **Data download status** field.

The following information may appear in the **Data download status** field:

Normal case:

- **Idle (0000)**. This information is sent if the terminal has transferred these configuration files without any error.
- **Disabled (0001)**: the Data Download Mode field is set to OFF.

Connection to FTP server failed:

- **ServerErr (0301):** error connecting to the FTP server (network cable disconnected, or bad FTP server IP address
- **LoginErr (0302):** Incorrect login (wrong login or password)
- **TransferError (0304):** Alarm received during transfer (transfer stopped)
- **NetworkErr (0305):** Access to the LAN impossible (wrong network configuration)
- **ConnectionErr (0306):** Access denied (wrong FTP port)

Problem with one or more configuration files:

- **FileNotFound (0501):** File or directory not found (RETR error)
- **FileMoveErr (0502):** Movement to a none-existing file or directory
- **TmNotAvail (0503):** File tm.config not available
- **TmNotComp (0504):** File tm.config not compatible
- **NoFileTrans (0505):** Downloading made but no file transferred

Problem writing the localdb file in FLASH:

- **FileOpenErr (0A00):** impossible to open localdb file
- **KeyErr (0A01):** Invalid format for this parameter
- **MemAllocErr (0A02):** Memory allocation error

Case of successful configuration file loading:

- **UploadComplete (0B00):** Configuration files successfully uploaded

### 2.20.3 THE TERMINAL IS LOCKED AND IS NO LONGER ACCESSIBLE VIA THE LAN.

If your terminal is no longer accessible via a ping or http command and the configuration file download phase fails, proceed as follows to restart your terminal with the factory settings.

1. ***Power off your terminal (by disconnecting the mains adapter or network cable if power supply to the terminal is automatic).***
2. ***Press the "C" key when the terminal is powered on and hold down this key until the "Boot Menu" appears on the screen.***
3. ***Press the "7" key to restore your terminal's factory settings.***



**ATTENTION : If the terminal is configured manually, all the terminal settings are lost and must be entered again.**

### 2.20.4 PRESS THE TERMINAL KEYS DOES NOT HAVE ANY EFFECT.

The idle screen is correctly displayed on the terminal when a key is pressed on the terminal (for example the **"Menu"**) foxkey, nothing happens (the terminal screen is not refreshed).

In this case, check that the configuration file tm.config.<TT>.<VN>.ftp has been correctly downloaded, especially by checking the value of the **Data download status** field and check that it is available in the FTP server storage directly.

<TT> = 60ip or 70ip or 80ip depending on terminal model

<VN> = current terminal software release (example: v2_10_21)

### 2.20.5 THE CONFIGURATION FILE SETTINGS ARE NOT TAKEN INTO ACCOUNT

To activate the parameters proposed in the configuration files, the line concerned in the configuration file should not any table, space, or comment.



**ATTENTION : The comment lines must contain the character # followed by a space.**

### 2.20.6 THE CONFIGURATION FILES ARE NOT DOWNLOADED.

Check the following points:

- Check that the Data Download Mode field is set to ON.
- Check that the FTP server is compatible with passive mode, and that it is set to this mode.
- Check that the configuration files are available in the FTP server storage area.
- Check the configuration of the switch connection port.
- Check that the FTP server IP address is know to the terminal and that it is correct. In the terminal web interface, the **Status** tab displays in the **FTP server** field the FTP server IP address with information about the negotiation mode.
  - Manual input or option negotiated via the configuration files
  - Option 66 negotiated with the DHCP server
  - Bootp nextserver option negotiated with the DHCP server
- Check that there is no FTP server connection failure (see Chapter 2.20.2).

## 2.21 INFORMATION MESSAGES ON THE MIVOICE 5300 IP PHONE SCREEN

The following information messages may appear on the MiVoice 5300 IP Phone screen.

### 2.21.1 DOWNLOAD FAILURE

This message appears in the terminal start phase in the following cases:

- no specific configuration file based on MAC or directory number (localdb.config.<MAC@>.ftp and/or localdb.config.<TN>.ftp
- no global configuration file (localdb.config.ftp)
- no terminal software or TM file (aamxip_vx_xx_xx.ftp, tm.config.<TT>.<VN>.ftp)

### 2.21.2 NET SETTINGS CHANGED, REBOOT NECESSARY

This message appears in the following cases:

- change of one or more network settings requiring the terminal to restart so it is taken into account (assigning a VLAN to the terminal, change of the VLAN priority, etc.).

### 2.21.3 SW UPDATE REQUIRED, UPDATING

This message appears in the following cases:

- Terminal restart order sent by the PBX to the terminal. This order results from an update of the following terminal settings:
  - FTP server connection settings
  - Settings concerning the terminal download policy (Software Download Mode, Data Download Mode, Name of the firmware to download, etc.).

**Note: This message appears when the software release or the global or specific configuration files of MiVoice 5300 IP Phone are updated via TMA.**

# 3 MITEL 6000 SIP PHONES

The MiVoice 6000 series SIP Phone consists of thirteen terminal types:

- Mitel 6730 SIP Phone,
- Mitel 6731 SIP Phone,
- Mitel 6735 SIP Phone,
- Mitel 6737 SIP Phone,
- Mitel 6739 SIP Phone,
- Mitel 6753 SIP Phone,
- Mitel 6755 SIP Phone,
- Mitel 6757 SIP Phone,
- Mitel 6863 SIP Phone,
- Mitel 6865 SIP Phone,
- Mitel 6867 SIP Phone,
- Mitel 6869 SIP Phone,
- Mitel 6873 SIP Phone.
- MiVoice 6920 IP Phone.
- MiVoice 6930 IP Phone.
- MiVoice 6940 IP Phone.

Mitel 6000 SIP Phones offer telephone communications over an IP network using SIP (session initiation protocol).

As of release 2.5.1.2000 of the firmware, Mitel 6730 SIP Phone, 6731 SIP, 6751 SIP, 6753 SIP, 6755 SIP and 6757 SIP Phones are compatible with the MiVoice 5000 solution:

- XS, XL, XD R5000.1 R5.1C N7 and later (official release)
- MiVoice 5000 R5000.1 R5.1C N7 and later (official release).

As of release 3.0.1.38 of the firmware, Mitel 6739 SIP Phone is compatible with the MiVoice 5000 solution:

- XS, XL, XD R5000.2 R5.2 AB and later (official release)
- MiVoice 5000 R5000.2 R5.2 AB and later (official release)

As of release 3.2.2 of the firmware, Mitel 6735 SIP Phone and 6737i  are compatible with the MiVoice 5000 solution:

- XS, XL, XD R5.3 SP1 and later (official release)
- MiVoice 5000 Server R5.3 SP1 and later (official release)

As of release 3.3.1 of the firmware, Mitel 6863 SIP Phone, 6865 SIP and 6867 SIP are compatible with the MiVoice 5000 solution:

- XS, XL, XD R6.1 and later (official release)
- MiVoice 5000 Server R6.1 and later (official release)

As of release 4.0.0 of the firmware, Mitel 6869 SIP Phone is compatible with the MiVoice 5000 solution:

- XS, XL, XD R6.1 SP1 and later (official release)
- MiVoice 5000 Server R6.1 SP1 and later (official release)

As of release 4.2.0 of the firmware, Mitel 6873 SIP Phone is compatible with the MiVoice 5000 solution:

- XS, XL, XD R6.2 and later (official release)

MiVoice 5000 Server R6.2 and later (official release)

As of release 5.0 of the firmware, Mitel 68920, 6930and 6940 IP phones is compatible with the MiVoice 5000 solution:

- XS, XL, XD R6.5 and later (official release)
- MiVoice 5000 Server R6.5 and later (official release)

**ATTENTION : The compatibility of SIP terminals with other PBX platforms cannot be guaranteed by Mitel and must be checked by our partners. The target PBX platform must be compatible with RFC 3261 of SIP.**

-

## 3.1 MITEL 6730 SIP PHONES



### 3.1.1 DESCRIPTION OF MITEL 6730 SIP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 3.1.2 SALES CODE FOR MITEL 6730 SIP PHONE

The sales code for Mitel 6730 SIP Phone with mains unit is A673001311051.

## 3.2 MITEL 6731 SIP PHONES



### 3.2.1 DESCRIPTION OF MITEL 6731 SIP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 3.2.2 SALES CODE FOR MITEL 6731 SIP PHONE

The sales code for Mitel 6731 SIP Phone without mains unit is A673101311055.

## 3.3 MITEL 6735 SIP PHONES



### 3.3.1 DESCRIPTION OF MITEL 6735 SIP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 3.3.2 SALES CODE FOR MITEL 6735 SIP PHONE

The sales code for Mitel 6735 SIP Phone without mains unit is A6735-0131-1055.

## 3.4 MITEL 6737 SIP PHONES



### 3.4.1 DESCRIPTION OF MITEL 6737 SIP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 3.4.2 SALES CODE FOR MITEL 6737 SIP PHONE

The sales code for Mitel 6737 SIP Phone without mains unit is A6737-0131-1055.

## 3.5 MITEL 6739 SIP PHONES



### 3.5.1 DESCRIPTION OF MITEL 6739 SIP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 3.5.2 SALES CODE FOR MITEL 6739 SIP PHONE

The sales code for Mitel 6739 SIP Phone without mains unit is A673901311055.

## 3.6 MITEL 6751 SIP PHONES



### 3.6.1 DESCRIPTION OF MITEL 6751 SIP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 3.6.2 SALES CODE FOR MITEL 6751 SIP PHONE

The sales code for Mitel 6751 SIP Phone with mains unit is A175101311055.

## 3.7 MITEL 6753 SIP PHONES





### 3.7.1 DESCRIPTION OF MITEL 6753 SIP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 3.7.2 SALES CODE FOR MITEL 6753 SIP PHONE

The sales code for Mitel 6753 SIP Phone with mains unit is A175301311055.

## 3.8 MITEL 6755 SIP PHONES





### 3.8.1 DESCRIPTION OF MITEL 6755 SIP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 3.8.2 SALES CODE FOR MITEL 6755 SIP PHONE

The sales code for Mitel 6755 SIP Phone with mains unit is A175501311055.

## 3.9 MITEL 6757 SIP PHONES





### 3.9.1 DESCRIPTION OF MITEL 6757 SIP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 3.9.2 SALES CODE FOR MITEL 6757 SIP PHONE

The sales code for Mitel 6757 SIP Phone with mains unit is A175701311055.

## 3.10 MITEL 6863 SIP PHONES





### 3.10.1 DESCRIPTION OF MITEL 6863 SIP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 3.10.2 SALES CODE FOR MITEL 6863 SIP PHONE

The sales code for Mitel 6863 SIP Phone **without mains unit** is 80C00005AAA-A.

## 3.11 MITEL 6865 SIP PHONES





### 3.11.1 DESCRIPTION OF MITEL 6865 SIP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 3.11.2 SALES CODE FOR MITEL 6865 SIP PHONE

The sales code for Mitel 6865 SIP Phone **without mains unit** is 80C00001AAA-A.

## 3.12 MITEL 6867 SIP PHONES





### 3.12.1 DESCRIPTION OF MITEL 6867 SIP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 3.12.2 SALES CODE FOR MITEL 6867 SIP PHONE

The sales code for Mitel 6867 SIP Phone **without mains unit** is 80C00002AAA-A.

## 3.13 MITEL 6869 SIP PHONES



### 3.13.1 DESCRIPTION OF MITEL 6869 SIP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 3.13.2 SALES CODE FOR MITEL 6869 SIP PHONE

The sales code for Mitel 6869 SIP Phone **without mains unit** is 80C00003AAA-A.

## 3.14 MITEL 6873 SIP PHONES



### 3.14.1 DESCRIPTION OF MITEL 6873 SIP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 3.14.2 SALES CODE FOR MITEL 6873 SIP PHONE

The sales code for Mitel 6873 SIP Phone **without mains unit** is 50006790.

## 3.15 POSTE MIVOICE 6920 IP PHONE



### 3.15.1 DESCRIPTION OF MIVOICE 6920 IP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 3.15.2 SALES CODE FOR MIVOICE 6920 IP PHONE

The sales code for MiVoice 6920 IP Phone **without mains unit** is 50006767.

## 3.16 POSTE MIVOICE 6930 IP PHONE



### 3.16.1 DESCRIPTION OF MIVOICE 6930 IP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 3.16.2 SALES CODE FOR MIVOICE 6930 IP PHONE

The sales code for MiVoice 6930 IP Phone **without mains unit** is 50006769.

# 3.17 POSTE MIVOICE 6940 IP PHONE



## 3.17.1 DESCRIPTION OF MIVOICE 6940 IP PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

## 3.17.2 SALES CODE FOR MIVOICE 6940 IP PHONE

The sales code for MiVoice 6940 IP Phone **without mains unit** is 50006770.

## 3.18 CONNECTING MITEL 6731 SIP PHONE, 6735 SIP, 6737I, 6751 SIP, 6753 SIP, 6755 SIP AND 6757 SIP

**Note : For the 6730 SIP model, see the next paragraph.**

To headset (optional) (not available on Mitel

To extension modules 536M and 560M (only for Mitel 6735 SIP, 6737 SIP, 6753 SIP, 6755 SIP and 6757 SIP



To the handset



PC port: this port is used to connect a second network device, in this case a PC.

LAN port: this port is used to connect the terminal to the lo-

Port for connecting the mains adapter (required only if the local area network does not

**Note : 6735 SIP and 6737 SIP phones are compatible with Class 2 POE. Therefore, in addition to a key expansion module, it is necessary to have power supply via a mains unit.**

**Note : 6735 SIP et 6737 SIP phones have a Gigabit switch with two 10/100/1000 base T ports for connecting a PC, and can be powered over the LAN (802.3 af).**

**Note : 6735 SIP and 6737 SIP phones have a Gigabit switch with two 10/100/1000 base T ports for connecting a PC, and can be powered over the LAN (802.3 af).**

**Note : The Ethernet port labelled "PC" does not supply power online via other network devices.**

**Note : The mains adapter and PoE (via the local area network or online power adapter PoE) can be connected simultaneously and thus allow redundancy.**

**Note : 6735 SIP and 6737 SIP phones have optimised hardware for HD audio quality (handset and loudspeaker).**

**Note : 6735 SIP and 6737 SIP phones are supplied without mains unit. This latter must be ordered separately.**

### 3.18.1 HEADSET SOCKET WIRING OF TERMINALS MITEL 6000 SIP PHONES




The sales code for the DHSG cable used with 6735 SIP, 6737 SIP, 6753 SIP, 6755 SIP, 6757 SIP, 6865 SIP, 6867 SIP and 6869 SIP phones is D006200113400.

## 3.19 CONNECTING MITEL 6730 SIP PHONE

Unlike the other models of this range, 6730 SIP phone does not have the following features:

- Headset connection,
- Extension module connection,
- Power over Ethernet (PoE). This terminal can only be powered via the accompanying mains unit (5 VCC, 2 A).

## 3.20 CONNECTING MITEL 6863 SIP PHONE

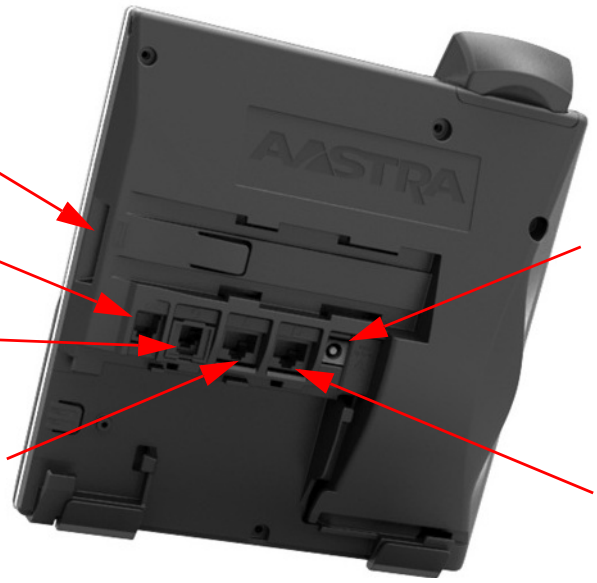



**Note : 6863 SIP phone is compatible with POE Class 1 (~3.84W). This terminal does not have any headset socket. No extension module can be connected to this terminal.**

**Note : 6863 SIP phones have a switch with two 100 base T ports for connecting a PC, and can be powered over the LAN (802.3 af).**

**Note : 6863 SIP phones are supplied without any mains unit. This latter must be ordered separately, if necessary.**

## 3.21 CONNECTING MITEL 6865 SIP PHONE




**Note : 6865 SIP phone is compatible with POE Class 2 (~6.49W).**

**Note : Up to three extension modules M680i or M685i can be connected to 6865 SIP phones (with PoE Class 2).**

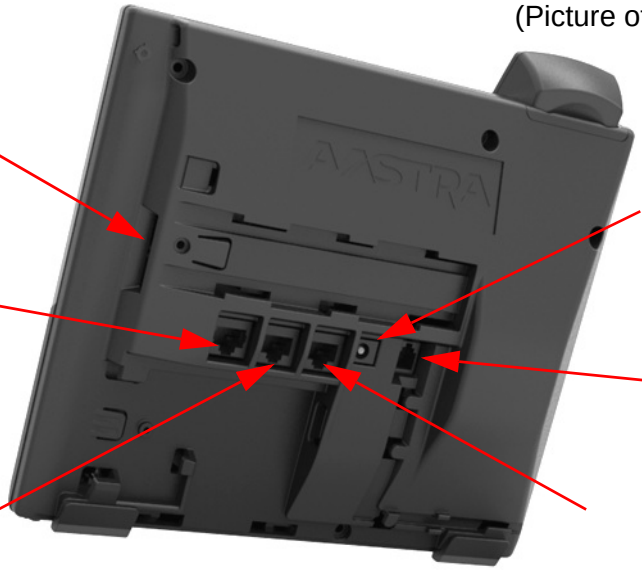
**Note : 6865 SIP phones have a Gigabit switch with two 100/1000 base T ports for connecting a PC, and can be powered over the LAN (802.3 af).**

**Note : 6865 SIP phones have optimised hardware for HD audio quality (handset and loudspeaker).**

**Note : 6865 SIP phones are supplied without any mains unit. This latter must be ordered separately, if necessary.**

## 3.22 CONNECTING MITEL 6867 SIP PHONE / 6869 SIP PHONES

(Picture of a 6867 SIP phone)




**Note : 6867 SIP and 6869 SIP phones are compatible with Class 2 POE (~6.49W).**

**Note : Up to three extension modules M680i or M685i can be connected to 6867 SIP or 6869 SIP phones (with dynamic negotiation of PoE Class 3 once an extension module is connected).**

**Note : 6867 SIP and 6869 SIP phones have a Gigabit switch with two 100/1000 base T ports for connecting a PC, and can be powered over the LAN (802.3 af).**

**Note : 6867 SIP and 6869 SIP phones have optimised hardware for HD audio quality (handset and loudspeaker).**

**Note : 6867 SIP and 6869 SIP phones are supplied without mains unit. This latter must be ordered separately, if necessary.**

## 3.23 CONNECTING MITEL 6873 SIP PHONES

**Note : 6873 SIP phone is compatible with POE Class 3 (~12.95W).**

**Note : Up to three extension modules M680i or M685i can be connected to 6873 SIP phones (with dynamic negotiation of PoE Class 4 once an extension module is connected).**

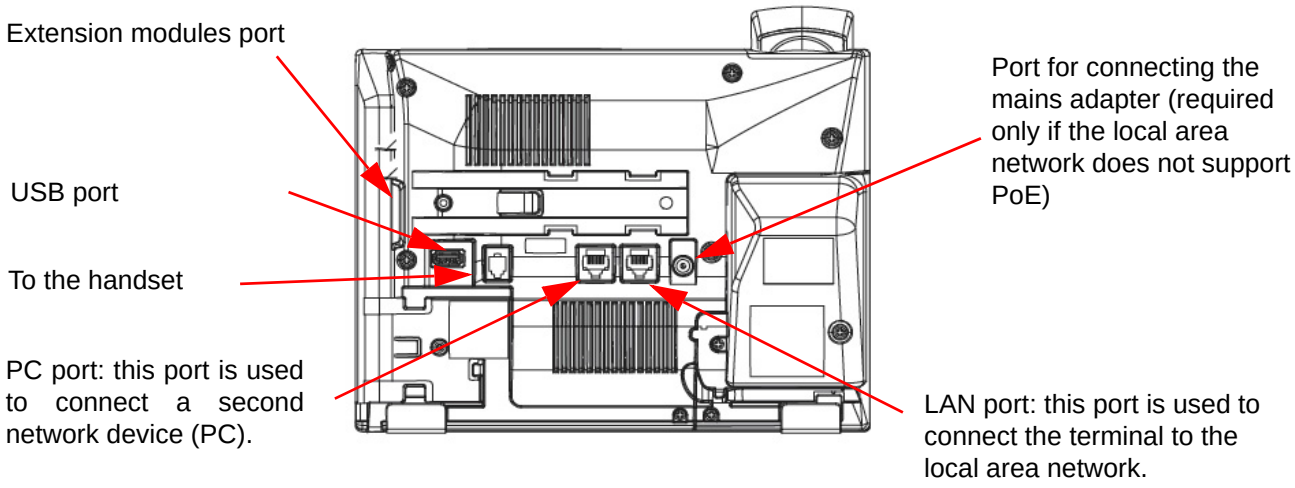
**Note : 6873 SIP phones have a Gigabit switch with two 100/1000 base T ports for connecting a PC, and can be powered over the LAN (802.3 af).**

**Note : 6873 SIP phones have optimised hardware for HD audio quality (handset and loudspeaker).**

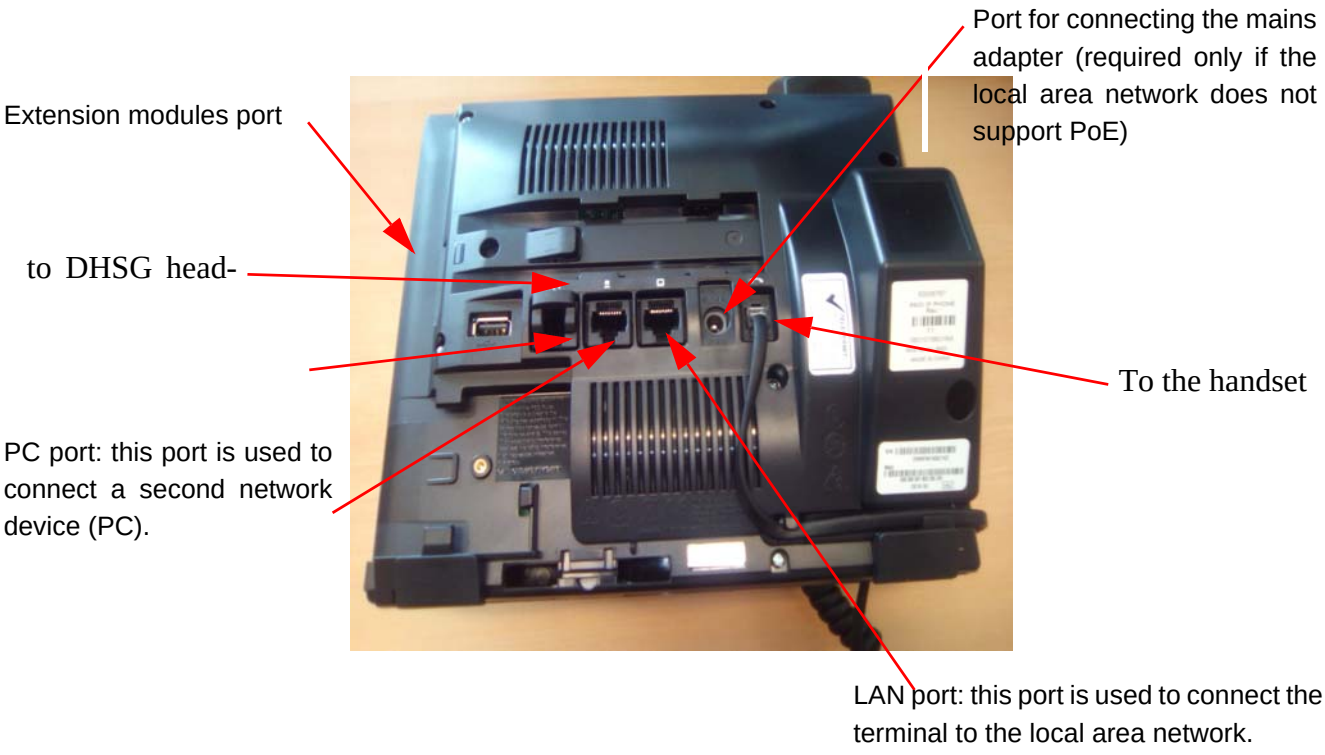
**Note : 6873 SIP phones have a USB port, for connecting a headset.**

**Note : 6873 SIP phones have an integrated bluetooth module, for connecting a headset.**
**A DHSG headset cannot be connected to 6873 SIP phones.**

**Note : 6873 SIP phones are supplied without any mains unit. This latter must be ordered separately, if necessary.**



## 3.24 CONNECTING MIVOICE 6920 IP PHONES




**Note : 6920 IP phone is compatible with POE classe 2 (~6.49W).**

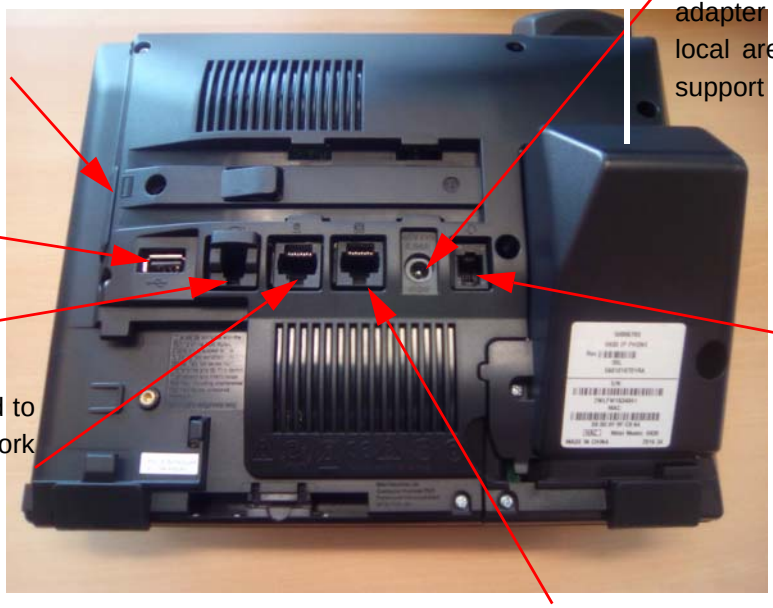
**Note : Up to three extension modules M695 can be connected to 6920 IP phone (with dynamic negotiation of PoE Class 3 once an extension module is connected).**

**Note : 6920 IP phones phones have a Gigabit switch with two 100/1000 base T ports for connecting a PC, and can be powered over the LAN (802.3 af).**

**Note : 6920 IP phones have optimised hardware for HD audio quality (handset and loudspeaker).**

**Note : 6920 IP Phones are supplied without any mains unit. This latter must be ordered separately, if necessary.**

## 3.25 CONNECTING MIVOICE 6930 IP PHONES




**Note : 6930 IP phone is compatible with POE classe 2 (~6.49W).**

**Note : Up to three extension modules M695 can be connected to 6930 IP phone (with dynamic negotiation of PoE Class 3 once an extension module is connected).**

**Note : 6930 IP phones phones have a Gigabit switch with two 100/1000 base T ports for connecting a PC, and can be powered over the LAN (802.3 af).**

**Note : 6930 IP phones have optimised hardware for HD audio quality (handset and loudspeaker).**

**Note : 6930 IP Phones are supplied without any mains unit. This latter must be ordered separately, if necessary.**

## 3.26 CONNECTING MIVOICE 6940 IP PHONES

**Note : 6940 IP phone is compatible with POE Class 3 (~12.95W).**

**Note : Up to three extension modules M695 can be connected to 6940 IP phones (with dynamic negotiation of PoE Class 4 once an extension module is connected).**

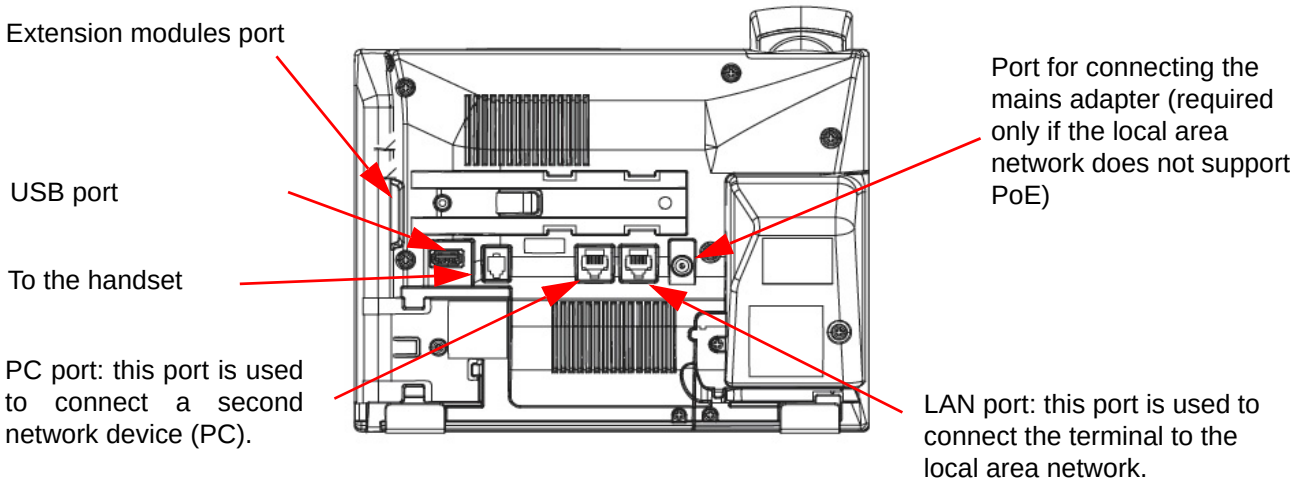
**Note : 6940 IP phones have a Gigabit switch with two 100/1000 base T ports for connecting a PC, and can be powered over the LAN (802.3 af).**

**Note : 964 IP phones have optimised hardware for HD audio quality (handset and loudspeaker).**

**Note : 6940 IP phones have a USB port, for connecting a headset.**

**Note : 6940 IP phones have an integrated bluetooth module, for connecting a headset.**
**A DHSG headset cannot be connected to 6940 IP phones.**

**Note : 6940 IP phones are supplied without any mains unit. This latter must be ordered separately, if necessary.**



## 3.27 EXPANSION MODULES

**Note : Not applicable to 6730 SIP, 6731 SIP, 6751 SIP and 6863 SIP phones.**

- Two extension modules are available and can be used on Mitel 6735 SIP Phone, 6737 SIP, 6753 SIP, 6755 SIP and 6757 SIP phones:
  - The sales code for expansion module M670i is A173600001055.
  - The sales code for expansion module M675i is A176000001055.
- One extension module is available and can be used on Mitel 6865 SIP Phone, 6867 SIP, 6869 SIP and 6873 SIP phones:
  - The sales code for expansion module M680i is 80C00010AAA-A.
- One extension module is available and can be used on Mitel 6865 SIP Phone, 6867 SIP, 6869 SIP and 6873 SIP phones:
  - The sales code for expansion module M685i is 80C00007AAA-A.
- One extension module is available and can be used on MiVoice 6920 IP Phone, 6930 IP, and 6940 IP:
  - The sales code for expansion module M695 is 50006874.

### 3.27.1 EXPANSION MODULE M670I

- Up to 3 modules per terminal
- Direct power supply from the terminal
- 36 programmable keys, with associated LEDs (line, dial, Do not Disturb, etc.)

**Compatible with Mitel 6735 SIP Phone, 6737i, 6753 SIP, 6755 SIP, 6757 SIP and 6739 SIP phones**





### 3.27.2 EXPANSION MODULE M675I

- Up to 3 modules per terminal
- Direct power supply from the terminal
- 60 programmable keys, with associated LEDs (line, dial, Do not Disturb, etc.)
- Compatible with Mitel 6735 SIP Phone, 6737 SIP, 6755 SIP, 6757 SIP and 6739 SIP phones





### 3.27.3 EXTENSION MODULE M680I

- Up to 3 modules per terminal
- Direct power supply from the terminal
- PoE Class 2 maintained on 6865 SIP phone with three modules connected
- Changeover to PoE Class 3 once a module is connected to 6867 SIP phones
- Changeover to PoE Class 4 once a module is connected to 6873 SIP phones
- By default, 6869 SIP phones are always in Class 3.
- 16 programmable keys, with associated LEDs (line, dial, Do not Disturb, etc.)
- Compatible with Mitel 6865 SIP Phone, 6867 SIP, 6869 SIP et 6873 SIP phones
- Cannot be used with M685i





### 3.27.4 EXTENSION MODULE M685I

- Up to 3 modules per terminal
- Direct power supply from the terminal
- PoE Class 2 maintained on 6865 SIP phone with three modules connected
- Changeover to PoE Class 3 once a module is connected to 6867 SIP phones
- Changeover to PoE Class 4 once a module is connected to 6873 SIP phones
- By default, 6869 SIP phones are always in Class 3.
- 3 pages of 28 programmable keys, with associated LEDs (line, dial, Do not Disturb, etc.)
- Compatible with Mitel 6865 SIP Phone, 6867 SIP, 6869 SIP et 6873 SIP phones
- Cannot be used with M680i



### 3.27.5 EXTENSION MODULE M695

- Up to 3 modules per terminal
- Direct power supply from the terminal
- PoE Class 2 maintained on 6920 IP phone with three modules connected
- Changeover to PoE Class 3 once a module is connected to 6930 IP phones
- Changeover to PoE Class 4 once a module is connected to 6940 IP phones
- By default, 6940 IP phones are always in Class 3.
- 3 pages of 28 programmable keys, with associated LEDs (line, dial, Do not Disturb, etc.)
- Compatible with MiVoice 6900 IP phones

## 3.28 DETACHABLE MAGNETIC KEYPAD K680I

- Easy text input
- Direct power supply from the terminal
- No cable
- Connection to the terminal is through magnetic contact.
- Compatible with Mitel 6867 SIP Phone, 6869 SIP phone and 6930 IP phone
- The keypad exists in three versions with different sales codes:
  - QWERTY whose sales code is 80C00008AAA-A
  - AZERTY whose sales code is 80C00014AAA-A
  - QWERTZ whose sales code is 80C00013AAA-A.



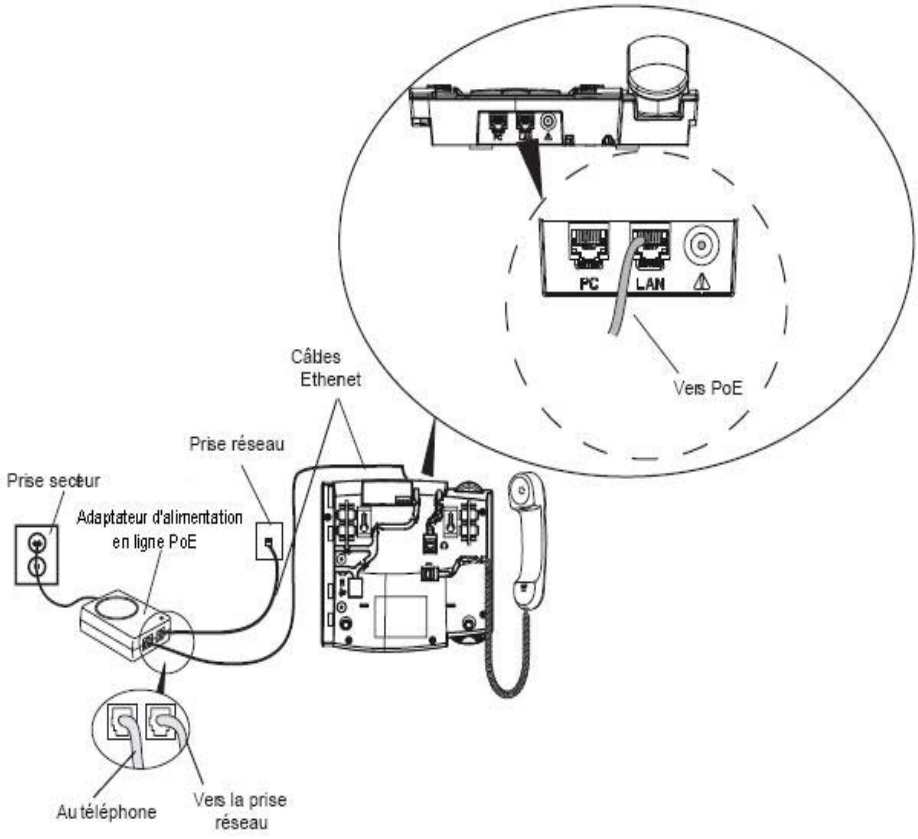


## 3.29 OPTIONAL ACCESSORIES

**Note : Not applicable to 6730 SIP phones.**

An online PoE (Power over Ethernet) adapter is used to power up the terminal if the LAN switch is not 802.3af compatible and cannot be used to directly power up the terminal online on its LAN port, and if the mains adapted delivered with the terminal is not used.

This adapter supplies 48 volts to terminal 675xi via the Ethernet cable on contacts 4 & 5 and 7 & 8. Do not use this adapter to power up other devices. This adapter is available for Mitel 6735 SIP Phone, 6737 SIP, 6751 SIP, 6753 SIP, 6755 SIP and 6757 SIP phones.




**Note : Mitel 6000 SIP Phones support online power supply over the Ethernet cable, either on the two active pairs (1-2, 3-6), or on the two inactive pairs (4-5, 7-8), but not simultaneously.**

The sales code for the online PoE adapter without power cable is: D00230031PS00

The sales code for the online PoE adapter cable is: 20260511

A mains adapter is used to power up the terminal if the LAN switch is not 802.3af compatible and cannot be used to directly power up the terminal online on its LAN port.

This adapter supplies 48V to Mitel 6000 SIP Phones. Do not use this adapter to power up other devices.

- The sales code for the Mitel 6700 SIP Phone is D002310510075.
- The sales code for the Mitel 6800 SIP Phone power unit is D002310510075.

**Note : This power supply unit is compatible with Mitel 6700 SIP Phones.**

## 3.30 TELEPHONY FEATURES OF MITEL 6000 SIP PHONES

See the product guide for this terminal range.

## 3.31 MIVOICE 5000 ARCHITECTURES WITH MIVOICE 6000 SIP PHONES

Mitel 6000 SIP Phones are declared in the system (MiVoice 5000 Server or Mitel 5000 Gateways), and connect via the SIP service integrated into the UCV card of Mitel 5000 Gateways or via the SIP service integrated into MiVoice 5000 Server.

These terminals support the login site optimisation function. This enables the phone to register with the SIP service of a site which may be different from the site on which the terminal subscription is declared.

Mitel 6000 SIP Phones are declared either on a ToIP VLAN dedicated to terminals, or they are used both on a Data VLAN and ToIP VLAN in 802.1Q if the PC is connected to the terminal.

The FTP server used for downloading on Mitel 6000 SIP Phone (firmware and configuration files) may be hosted by:

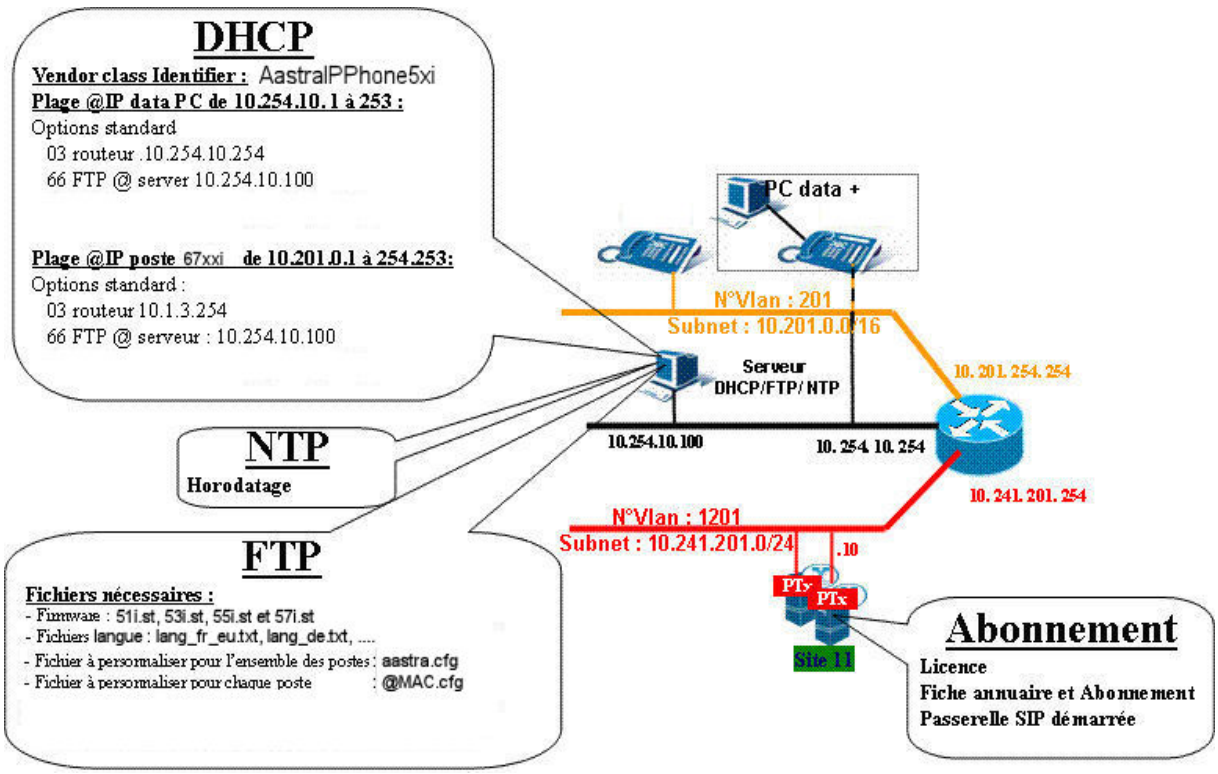
- **a Windows 2000/2003 Server platform** (under the network administrator's responsibility),
- **a MiVoice 5000 Server** (under the network administrator's responsibility),
- **Mitel 5000 Gateways**. In this case, the FTP server is integrated into the UCV card, and the corresponding service will be fully managed by the system.

For each terminal, the FTP server address used must be declared:

- Either through manual configuration (directly on the terminal or via the web interface),
- Or by configuring the DHCP server.

One DHCP server, for supplying the IP address, must be accessible from the ToIP VLAN.

The 3-level Ethernet switch (router in general) handles the inter-VLAN routing, as well as DHCP relay for non-VLAN Data devices.



## 3.32 MITEL 6000 SIP PHONE CONFIGURATION MODES

The different configuration modes of Mitel 6000 SIP phones are:

- For a single-site configuration, from the integrated TMA (Menu **Terminal service**) on Mitel 5000 Gateways and MiVoice 5000 Server,
- For a multi-site configuration, from the TMA installed on MiVoice 5000 Manager (Menu **Terminal service** in the **Terminal management** column),
- Manual mode through direct access in the terminal menus,
- Manual mode via the terminal management WEB interface.

**Modes recommended according to configuration:**

- **In a single-site Mitel 5000 Gateways configuration**

  Mitel recommends configuring the terminals from the integrated TMA on MiVoice 5000 also using the integrated FTP and DHCP services.

  - **During a first installation:**

    Deployment may be automatic during start in STANDARD or TOTAL mode, using CTRL + i. Refer to Section “Managing terminals with the TMA integrated into MiVoice 5000” on page 101.

  - **During iPBX update:**

    The terminals are automatically updated.

    The new iPBX software release also contains the new software releases associated with the terminals. Refer to Section “Managing terminals with the TMA integrated into MiVoice 5000” on page 101.

- **In a multi-site configuration**

  In a multi-site configuration containing several sites or multi-sites, one or more external DHCP servers or one or more external FTP servers, the use of the TMA integrated into MiVoice 5000 Manager is highly recommended. This application allows software update, global and specific data update for Mitel 6000 SIP Phones, without any manual operation on the phones. Refer to Section 7. “Managing terminals with TMA hosted by MiVoice 5000 Manager” on page 195

- **In case of manual configuration**

  To quickly deploy some terminals, direct configuration on the terminal or via the web interface may be envidsaged. Refer to Section 17. “Appendix 6: Manual configuration of MITEL 6000 SIP PHONES” on page 369

- **If TMA is not available**

  Be it a simple or complex configuration, Mitel recommends configuring the terminals via an integrated or external DHCP server in order to automatically recover its standard network settings and manage those associated with the supplier class of Mitel 6000 SIP Phones, where necessary. The configuration is completed by downloading the software and configuration files associated with Mitel 6000 SIP Phones via an integrated or external FTP server, by manually placing these files in the appropriate storage directory.

## 3.32.1 CONNECTING THE DATA SWITCH

**Mitel 6000 SIP Phone with or without PC connection:**

In this configuration, the terminal is connected to a port that is "Terminals" and "Data" VLAN compatible: it must mark its frames in the "Terminals" VLAN. Traffic on the the Switch port is marked for the terminal and not for the PC.

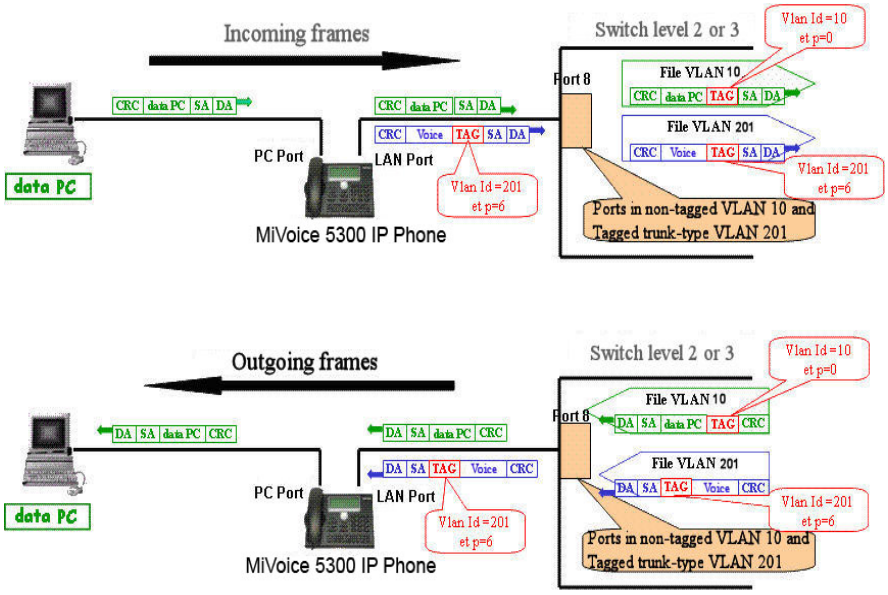
Mitel recommends configuring all the ports of the Switch to which some Mitel 6000 SIP Phones are connected in the same way, regardless of whether the terminal is standalone or connected with a PC. This way, the network administrator will not have to reconfigure the Switch ports based on PC availability or unavailability.

**Connecting the terminal:**

Connect the terminal to the switch port ("Terminals" + "Data" VLAN): the terminal will send its DHCP request on the "Data" VLAN and obtain its configuration, especially its VLAN ID, via the FTP server (firmware, language packs and configuration files) using a temporary IP address in the "Data" VLAN. The terminal will then restart on the "Terminals" VLAN. The terminal will send a second DHCP request on the "Terminals" VLAN an obtain its full configuration.

**Example of Ethernet frame marking on the switch port:**

check that the network socket for connecting to the Data switch actually belongs to the ToIP VLAN of Mitel 6000 SIP Phones and to the Data VLAN of the PCs.



## 3.33 CONFIGURING MITEL 6000 SIP PHONE FOR THE DUAL HOMING FUNCTION

The Dual Homing feature enables a terminal to connect to a backup site when the connection to its reference site is not possible, either because the reference site is out of service, or because its is not accessible via the network.

The diagram below gives an example of an architecture.




The settings to define on Mitel 6000 SIP Phones are:

- sip backup proxy ip => specifies the IP address of the backup site's SIP gateway
- sip backup proxy port => specifies the listening port of the backup site's SIP gateway
- sip backup registrar ip => specifies the IP address of the backup site's SIP gateway
- sip backup registrar port => specifies the listening port of the backup site's SIP gateway

These four settings can be defined through any of the following two methods:

- Via the global configuration file **aastra.cfg** or specific configuration file **<MAC>.cfg** depending on the client's network architecture (see Section 17.5.3). By default, these settings are defined in the file **aastra.cfg** while the corresponding lines are in comments.
- In manual configuration via the terminal configuration web interface (Menu **Advanced Settings > Global SIP > Basic SIP Network Settings**).

*See Section 17.5.2 for the priority given to the setting if this setting is defined using several methods.*

| Basic SIP Network Settings | |
|---|---|
| Proxy Server | 192.102.19.2 |
| Proxy Port | 5060 |
| Backup Proxy Server | 192.102.20.2 |
| Backup Proxy Port | 5060 |
| Outbound Proxy Server | 0.0.0.0 |
| Outbound Proxy Port | 0 |
| Registrar Server | 192.102.19.2 |
| Registrar Port | 5060 |
| Backup Registrar Server | 192.102.20.2 |
| Backup Registrar Port | 5060 |
| Registration Period | 3600 |
| Conference Server URI | |

**ATTENTION : Details about the working of the Dual Homing function and the configuration to be made on Web Admin or MiVoice 5000 Manager are given in the Multi-site Operating Manual (AMT/PTD/PBX/0081*).**

# 3.34 CONFIGURING MITEL 6000 SIP PHONE FOR THE MD5 AUTHENTICATION FUNCTION

## 3.34.1 WORKING PRINCIPLE:

The MD5 password is used to authenticate the Mitel 6000 SIP Phone which connects to MiVoice 5000 Server and Mitel 5000 Gateways. This MD5 password is defined in the MiVoice 5000 Server and Mitel 5000 Gateways subscription.

This control makes it possible to prevent the registration of another device that has the same directory number by mistake or maliciously.

This function is supported by Mitel 6000 SIP Phones as of V2.1.2.2005.

This control is made in the following cases:

- Each time the terminal is registered on the iPBX,
- Before each outgoing call.

**Note : There is no control on an incoming call.**

The MD5 password is defined both in Mitel 6000 SIP Phone and in the iPBX.

Mitel 6000 SIP Phone does not work in the following two cases:

- The MD5 password is different between Mitel 6000 SIP Phone and the iPBX.
- The MD5 password is defined in the iPBX but not in Mitel 6000 SIP Phone.

**Note : If the MD5 password is defined in Mitel 6000 SIP Phone but not in the iPBX, the terminal will be operational.**

## 3.34.2 CONFIGURING THE MD5 PASSWORD IN THE IPBX

To configure the MD5 password in the MiVoice 5000 Server and Mitel 5000 Gateways, proceed as follows:

- Go to the MD5 password definition menu:
  - this menu (124) is accessible via Subscribers / Subscriptions / Terminal authentication and MDP User Portal.
- Select the type of operation: **SIP authentication**
- Enter the First directory number.
- Enter the Last directory number.
- Select the creation mode:
  - Manual creation,
  - Automatic creation.

In case of manual creation, enter the MD5 password for the selected subscribers (alphanumeric code between 8 and 16 characters),

- Click the Confirm button to confirm the creation of MD5 password.

**Note : The Export operation is used to generate and save a file in .csv format containing the subscriptions and their MD5 password.**

**Note : Mitel OMM R2.1 type operation is used to generate and save a file in Mitel OMM R2.1 format containing the subscriptions and their MD5 passwords for DECT/IP radio fixed parts (see document AMT/PTD/PBX/0062* for the import mechanism of this file).**
**As of Mitel OMM 4.0 and R5.4, a daily or immediate data realignment mechanism from MiVoice 5000 to Mitel OMM 4.0 is used to automatically recover the MD5 password defined in the PBX for Mitel DECT/SIP radio fixed parts (Menu Subscribers > Rights > General parameters, Mitel OMM SIP management parameter application tab).**

It is possible to know whether a subscription has an already defined MD5 password.

This menu (1231) is accessible via Subscribers > Subscriptions > Characteristics: parameter **Terminal authentication** in the Characteristics tab.

### 3.34.3 CONFIGURING THE MD5 PASSWORD MANUALLY IN THE MITEL 6000 SIP PHONES

This configuration method must be used in the following cases only:

- Terminal service not started in Web Admin (single-site configuration)
- TMA not configured in MiVoice 5000 Manager (multi-site configuration)

The settings to define on Mitel 6000 SIP Phones are:

- **sip line1 password** => specifies the MD5 password used by Mitel 6000 SIP Phones
- **sip line1 auth name** => specifies the authentication name used by Mitel 6000 SIP Phones

This parameter can be defined using any of the three methods:

- Via the specific configuration file **<MAC>.cfg** (see Section 17.5.3). In this case, the lines **sip line1 password** and **sip line1 auth name** should not be in comment, while the line **sip line1 password** contains the MD5 password.
- In manual configuration via the terminal configuration menu (Menu **Options** > **Administrator Menu** > **SIP Settings** > **Password** et **Authentication Name**),
- In manual configuration via the terminal configuration web interface (Menu **Advanced Settings > line 1 > Basic SIP Authentication Settings > Password and Authentication Name**).

In multi-line configuration the setting to define is **sip lineN password** where **N**=line number 1 to 9.

**Note : See Section 17.5.2 for the priority given to the setting if this setting is defined using several methods.**

### 3.34.4 AUTOMATIC CONFIGURATION OF THE MD5 PASSWORD IN THE MITEL 6000 SIP PHONES

This configuration method must be used in the following cases only:

- Terminal service started in Web Admin (single-site configuration)
- TMA configured in MiVoice 5000 Manager (multi-site configuration)

Working principle:

Following the modification of the MD5 password in the iPBX (see Chapter 3.34.2), TMA is immediately notified by the management via the following two files:

- an action file,
- a modification description file containing the modified terminal and its new MD5 password.

These two files are either created by the iPBX if the terminal service is started in Web Admin, or by MiVoice 5000 Manager upon receiving an SNMP trap sent by the iPBX.

After this notification, TMA updates the specific configuration file of each terminal concerned with the right parameter and places this/these file(s) in the appropriate storage area on the FTP server (via a

symbolic link, in case of integrated FTP server). At the same time, an immediate specific data update action is sent to the terminal. This action results in the sending of a command by the iPBX (via NOTIFY messages) to update (in TLS configuration) or delete (in UDP configuration) the terminal's MD5 password then restart the terminal.

.



**ATTENTION : This mechanism is obsolete as R6.2. The password is directly sent to the terminal with a restart request.**



**Note : If Mitel 6000 SIP Phone is not accessible when this order is sent, the information is stored in the iPBX, and during the next terminal REGISTER, this order will again be sent to the terminal.**

When the terminal is restarted, the terminal retrieves its new specific configuration file containing information about the modifications made to its MD5 password (deletion, modification or creation). This information will only be taken into account by the terminal in UDP configuration (in TLS configuration, the priority associated with the settings requires sending NOTIFY messages to the terminal to update its MD5 password).



**ATTENTION : Manual deployment through free seating of a Mitel 6000 SIP Phone with a password defined in its subscription requires using TLS configuration. In this case, the password is sent to the terminal via some NOTIFY messages.**



**ATTENTION : In this operating mode, it should be impossible to enter the MD5 parameters via the TMA MMI. Therefore, ignore these parameters (sip line1 password and sip line1 auth name) during parameter distribution.**



**ATTENTION : Automatic MD5 password configuration is only available as of R5.2 SP1 (H2B).**



**ATTENTION : As of R5.4, in a multi-line configuration, the MD5 password is checked on the main multi-line subscription number only.**

# 3.35 CONFIGURING MITEL 6000 SIP PHONES IN THE 802.1X ENVIRONMENT

## 3.35.1 WORKING PRINCIPLE:

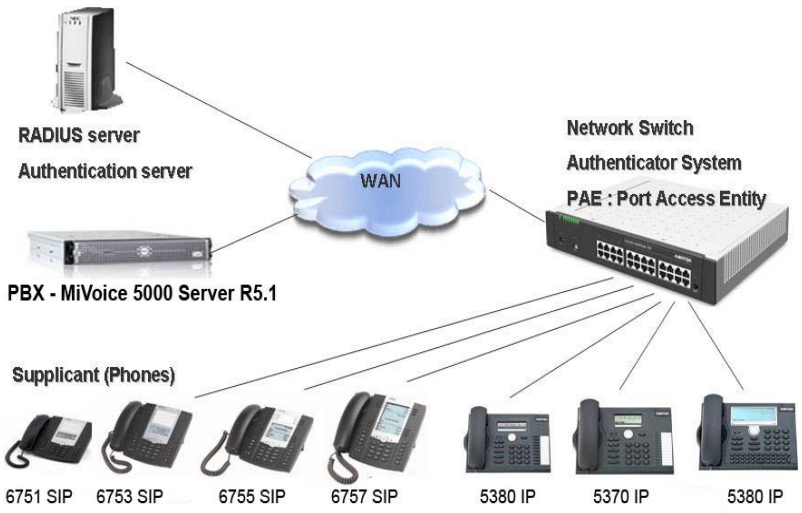
The purpose of Standard 802.1X is to authenticate to the network access during physical connection to the network. This authentication takes place before any self-configuration mechanism (for instance DHCP). In most cases, the service authorised in case of success is the Ethernet service.

The purpose of this standard is, therefore, only to validate a right to physically access the network, regardless of the transmission medium used, using some existing authentication mechanisms.

Three main players are involved in this mechanism:

- The system to authenticate (supplicant or client),
- The LAN access point (authenticator, switch, WiFi base station, etc.),
- The authentication server.

An example of 802.1X architecture is given below:




As long as he is not authenticated, the client cannot access the network; only authentication related exchanges are relayed to the authentication server via the access point. Once authenticated, the access point allows the client related traffic to flow.

The 802.1X protocol defines the use of EAP (Extensible Authentication Protocol, RFC3748), a mechanism that describes the authentication method.

Mitel 6000 SIP Phones are compatible with 802.1X authentication, in order to:

- authenticate them to a secure LAN according to the 802.1X protocol,
- allow transparent relay of the authentication request from a PC connected to the switch integrated into the terminal*

**ATTENTION : * This configuration works only on certain network devices (switch).**

### 3.35.2 CONFIGURING THE 802.1X AUTHENTICATION SETTINGS OF MITEL 6000 SIP PHONES

Mitel 6000 SIP Phones authenticate to the network with EAP-MD5.

Authentication is thus made using to two parameters: login and password.

The settings to define on Mitel 6000 SIP Phones are:

- **eap type:** 1 => specifies the protocol to be used (1=EAP-MD5)
- **identity:** xUsEr3 => specifies the 802.1X login
- **md5 password:** xPaSsWoRd3 => specifies the 802.1X password.

These settings can be defined through any of the following three methods:

- Via the specific configuration file **I<MAC>.cfg** (in Section 17.5.3). In this case, the two lines above must not be in comments and contain the type of protocol used, login and 802.1X password*.



**ATTENTION : * If the 802.1X authentication parameters are negotiated via the specific configuration files, the first update must be made on a network that does not implement 802.1x or on which it is deactivated.**

- Manual configuration via the terminal's configuration menu:
  - Menu **Options** > **Administrator Menu** > **Network Settings** > **Ethernet & VLAN** > **802.1X Settings** > **802.1X Mode**: **EAP-MD5**
  - Menu **Options** > **Administrator Menu** > **Network Settings** > **Ethernet & VLAN** > **802.1X Settings** > **EAP-MD5 Settings > Identity > User name**: enter the login.
  - Menu **Options** > **Administrator Menu** > **Network Settings** > **Ethernet & VLAN** > **802.1X Settings** > **EAP-MD5 Settings > MD5 Password > Password**: enter the password.
- Manual configuration via the terminal's configuration web interface:
  - Menu **Advanced Settings > 802.1X Support > EAP Type > EAP-MD5**
  - Menu **Advanced Settings > 802.1X Support > identity**: enter the login.
  - Menu **Advanced Settings > 802.1X Support > MD5 Password**: enter the password.

*See Section 17.5.2 for the priority given to the setting if the settings are defined using several methods.*

### 3.35.3 MITEL 6000 SIP PHONE AUTHENTICATION PROCEDURES

The normal authentication is procedures are as follows;

- The switch port is closed.
- Mitel 6000 SIP Phone is physically connected to the switch port.
- The switch sends an authentication request to Mitel 6000 SIP Phone then to the RADIUS server.
- The switch port is opened.
- Mitel 6000 SIP Phone connects to the LAN (ARP, DHCP, etc.).

### 3.35.4 SWITCH BEHAVIOUR

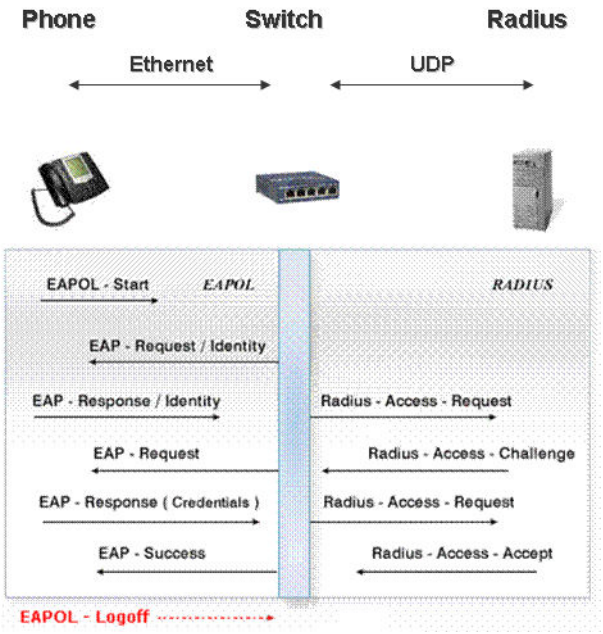
- The switch port remains closed in case of error or no response during authentication.
- A fresh authentication is started by the switch in case of error or no response to the previous authentication.
- The switch detects the terminal connection or disconnection to start authenticating the terminal.
- If the switch port is closed, new authentication attempts are made after terminal disconnection then reconnection.

### 3.35.5 BEHAVIOUR OF MITEL 6000 SIP PHONES

The authenticator (switch) generally initiates the communication once the port becomes active and sends an EAP request frame. If the authenticator does not initiate the communication, Mitel 6000 SIP Phones can initiate it by sending an EAP start request.

Mitel 6000 SIP Phone responds to re-authentication frames (every hour). The re-authentication mechanism can be executed during the communication phase.

The exchanges are illustrated on the following diagram:



## 3.36 CONFIGURING MITEL 6000 SIP PHONES FOR SIGNAL AND VOICE ENCRYPTION

See the call encryption operating manual (AMT/PTD/PBX/0103*).

## 3.37 CONFIGURING MITEL 6000 SIP PHONES FOR THE MULTI-LINE AND MULTI-CCOS FUNCTION

This function is available as of R5.4

See Mitel 6000 SIP Phone Configuration Manual for the multi-line and multi-CCOs function (AMT/PTD/PBX/0129*).

## 3.38 CONFIGURING MITEL 6000 SIP PHONES FOR THE BLF FUNCTION

### 3.38.1 WORKING PRINCIPLE:

This function is used to supervise the status of one or more other Mitel 6000 SIP Phones through LEDs. Each Mitel 6000 SIP Phone declared in an intercom group sends its status to the other terminals of the group, which have subscribed to the BLF service.

It is possible to supervise the calls in a simple or restricted intercom group (which does not allow calls to be picked up or made) via programmable keys. The other intercom types are not available.

Mitel 6000 SIP Phones can supervise all terminal types, except H323, ISDN terminals and hunt groups.

The supervising terminal must be logged on to minimum R5.2 and can supervise all the terminals (except the restrictions mentioned in the previous item), even those logged on to a release below R5.2.

**ATTENTION : See document AMT/PTD/PBX/0129 for the configuration of the BLF function of a multi-line subscription as of R5.4.**

### 3.38.2 PROGRAMMING THE BLF FUNCTION FOR A MITEL 6000 SIP PHONE

The BLF function requires programming:

- a programmable key in the intercom type Web Admin,
- a BLF key in the Mitel 6000 SIP Phone web interface.

Moreover, to be able to supervise or be supervised, Mitel 6000 SIP Phone must be assigned one or two CIGs.

#### *3.38.2.1 Programming one or two CIGs on Mitel 6000 SIP Phones*

These operations must be performed from Web Admin.

On a Mitel system in a single-site configuration, open the multi-site operation to assign the subscriptions one or two CIGs:

- Go to Menu Telephony Service > System > Configuration > Services then tick multi-site management.

Define the CIGs:

- Go to Menu Telephony Service > Subscribers > Hunt groups and companies > Intercom groups > Name, and define the CIG name.

For each subscription assigned to a Mitel 6000 SIP Phone, assign one or two CIGs:

- Go to Menu Telephony Service > Subscribers > Subscriptions > Characteristics, and assign one or more CIGs.

#### 3.38.2.2 *Programming an intercom type programmable key in Web Admin*

This operation must be performed from Web Admin.

- Go to Menu Telephony Service > Subscribers > Subscriptions > Characteristics, then in the Keys tab,
- Define a key with the following programming:
  - Programming type: Subscriber supervision or filtered call supervision
  - Parameter: indicate the subscription number to supervise
  - Signal: indicate the type of signal (CHUT, 1BEEP, BEEPS, RING)
  - Protected key: tick or untick
- Then validate the programming.

#### 3.38.2.3 *Programming the BLF function for a Mitel 6000 SIP Phone*

This operation must be performed from the Mitel 6000 SIP Phone web interface.

- Go to Menu Management mode > Display and XML keys.
- Define a key with the following programming:
  - Type: BLF
  - Label: indicate the label which must appear on the Mitel 6000 SIP Phone screen.
  - Value: indicate the subscription number to supervise.
  - Line: leave line 1 by default.
- Then validate the programming.



**ATTENTION : The operation chronology must be respected. Otherwise, it may be necessary to restart Mitel 6000 SIP Phone so the BLF function can work.**

# 3.39 RESTORING THE FACTORY SETTINGS OF MITEL 6000 SIP PHONES

## 3.39.1 FROM THE TERMINAL

Press the "Options" key.

- Press the "Options" key.
- In the options list, select the parameter: "Administrator Menu" then press "Select".
- Enter the administrator's password (22222) then press "Enter" to confirm.
- Select "Factory default" then press "Select".
- Press "Defualt" then "Restart" to restart the terminal.

## 3.39.2 FROM THE WEB INTERFACE

Procedure:

- Connect as Administrator.
- In Menu "Operation> Reset", click "Remove'" to delete the local configuration parameters.
- Then click "Restore" to reset the terminal with the default factory settings.
- Restart the terminal to take the operation into account: click <Restart>.

## 3.40 NTP SERVER

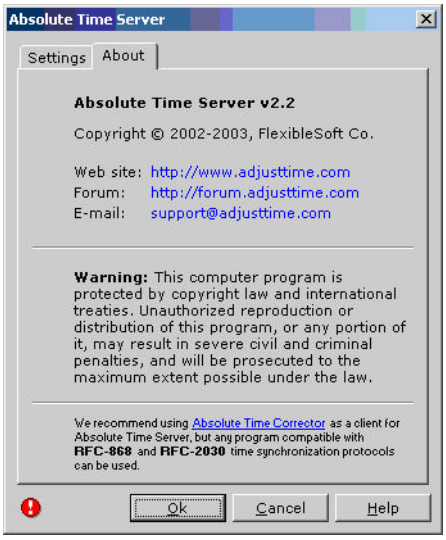
Time is set on the terminals via an NTP server. The NTP server IP address must be configured in the general settings (file **aastra**.cfg) or specific settings (file @MAC.cfg) of the SIP terminals.

The NTP server address can also be negotiated with the DHCP server via Option 42.

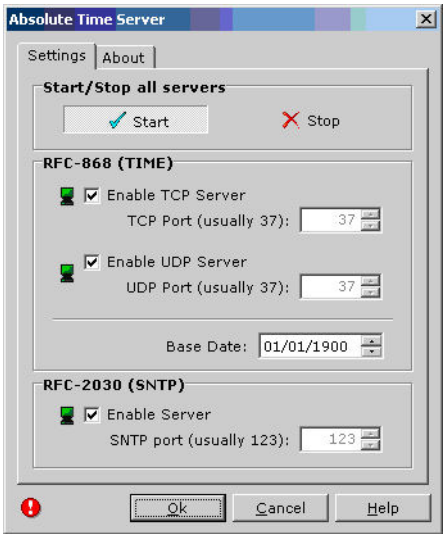
The available default NTP server on Mitel 5000 Gateways can be used.

The address of an external NTP server will be indicated in Menu System > Info > Date and time. This configuration allow the user to have the same reference time for Mitel 5000 Gateways as well as for Mitel 6000 SIP Phone and MiVoice 5300 IP Phone.

Example of NTP server: Absolute Time Server 2.2.




By default the server proposes the UDP and TCP 37 as well as the SNTP 123 port. These ports may be user-defined. The SIP phone uses SNTP 123 port.



# 3.41 CONFIGURATION REQUIRED IN THE SYSTEM

## 3.41.1 DECLARING MITEL 6000 SIP PHONES IN THE SYSTEM

Using Mitel 6000 SIP Phones requires unlocking the PROPRIETARY AUDIO licence. The type of subscription to be declared for Mitel 6000 SIP Phones is "Internal Subscriber".

Procedure:

- Go to the licence selection menu:
  - this menu (123) is accessible from System / Info / Licences.
- Enter the unlocking key corresponding to the number of Mitel 6000 SIP Phones deployed on the client's local area network.
- Create internal subscriber type subscriptions (LOCAL SUB).
  - This menu (121) is accessible via Subscribers / Subscriptions / Creation.

## 3.41.2 CONFIGURING THE ENCODING LAWS ASSOCIATED WITH MITEL TERMINALS MITEL 6000 SIP PHONES

- Go to the encoding law selection menu:
  - this menu (441) is accessible via Network and Links / Quality of service / Voice over IP encoding law.

Select the type of call: INTERNAL

Select the type of terminal: SIP

**Note : The SIP type corresponds to Mitel 6000 SIP Phones and other commercially available functional SIP phones.**

- Confirm by clicking the "Select item" button. In the next menu, indicate the encoding law you want according to the available bandwidth and the voice quality required.
- Then check the application of the encoding laws:

Go to the encoding law display menu:

- this menu (442) is accessible via NETWORK AND LINKS / Quality of service / Display encoding laws.

## 3.42 CONFIGURING THE ETHERNET SWITCH

According to the general recommendations on the MiVoice 5300 solution, a VLAN cutting must be used:

- A VLAN comprising the PT2/IPS cards and MiVoice 5000 Servers,
- One or more VLANs containing some Mitel 6000 SIP Phones
- A VLAN containing the telephony servers (messaging, administration, etc.)
- One or more set of VLAN Data

Standalone terminals:

| TERMINAL CONFIGURATION (WEB INTERFACE/ AASTRA.CFG) | CONFIGURING THE ETHERNET SWITCH |
|---|---|
| VLAN Enabled (no) / tagging enabled=0 | The Ethernet switch port is in a "Terminals" VLAN without 802.1Q marking. |
| VLAN Enabled (yes) / tagging enabled=1<br>Port 0 VLAN ID 20 / VLAN id: 20 | The terminal and Ethernet switch mark the frames in 802.1Q on VLAN 20. |

Terminals with a PC connection:

| TERMINAL CONFIGURATION (WEB INTERFACE/ AASTRA.CFG) | CONFIGURING THE ETHERNET SWITCH |
|---|---|
| VLAN Enabled (yes) / tagging enabled=1<br>Port 0 VLAN ID 20 / VLAN id: 20<br>Port 1 VLAN ID 30 / VLAN id port 1: 30 | The terminal and Ethernet switch mark the frames in 802.1Q on VLAN 20. The frames to the PC are marked in VLAN 30, Mitel 6000 SIP Phone manages the marking to the PC.<br>Using VLAN 4095 on port 1 allows all the unmarked frames to be sent to the PC port. This configuration is recommended because the DATA flow marking may not be compatible with certain routers. |

## 3.43 QOS ON THE IP NETWORK

Mitel 6000 SIP Phones can mark the ToIP frames according to their type (signalling, RTP, RTCP) on level 2 (802.1Q) and on level 3 (DiffServ).

They can also assign a level 2 priority to traffic from the connected PC.

Level 2 devices must not modify the marking of the traffic from Mitel 6000 SIP, unless there is an incoming traffic analysis and traffic marking.

On level 3, just activate DiffServ in the devices to take account of the ToIP frames.

The usual QoS recommendations are:

- Level 2 priority ToIP (signalling, RTP/RTCP)=6
- Level 2 priority Data=0
- Level 3 priority ToIP (RTP/RTCP flow)=B8h
- Level 3 priority ToIP (signalling flow)=A0h
- Level 3 priority Data=00h

# 3.44 TROUBLESHOOTING SOLUTIONS

## 3.44.1 WHY DOES MY MITEL 6000 SIP PHONE DISPLAY "APPLICATION MISSING"?

If you have encountered some network problems while Mitel 6000 SIP Phone was downloading the firmware from the FTP server, it is possible that the phone is longer able to retrieve the firmware. If Mitel 6000 SIP Phone is no longer able to communicate with the FTP server while trying to download the firmware again and it cannot locate the firmware locally, the message "Application missing" appears.

Mitel 6000 SIP Phone also displays the following text: "Recovery web-client at: <IP Address>".

The IP address is the phone's IP address. If the phone cannot receive an IP address from the DHCP server or has lost its static IP address, the phone automatically obtains the default IP address 192.168.0.50.

To retrieve the firmware for your phone in this case, proceed as follows:

1. Open the web browser on a PC located on the same network as the terminal.
2. In the URL type: "http:// <IP address>" (where the IP address is the IP address displayed on the phone). The browser opens the Mitel IP terminal firmware recovery page.
3. Recover and copy the firmware which corresponds to the terminal model in the FTP server storage area, if necessary.
4. Enter the FTP server IP address of the terminal model.
5. Click "Download firmware" then wait till the end of the downloading operation.

At the end of the terminal download, the password recover their default value:

Admin: 22222 Administrator access

User: "no password" for user access.



**ATTENTION : During the recovery procedure and as long as it has not been reloaded by its configuration files, the terminal does not mark the frames in 802.1Q (VLAN number). It may be necessary, for instance if the terminal is connected to a PC and is using 802.1Q marking, to temporarily move on a port of the IP network in "access" mode.**



**ATTENTION : In "recovery" mode, the terminal no longer has any default router: the PC and FTP server must be on the same IP network as the terminal.**

## 3.44.2 WHY DOES MY MITEL 6000 SIP PHONE DISPLAY "NO SERVICE"?

The phone displays "No service", especially if the SIP parameters have not been correctly defined. If the IP address of the parameter "Registrar server" is not entered correctly, the terminal will not be able to register with the SIP access point of the MiVoice 5000 Server or Mitel 5000 Gateways platform and will display the message "No service".

The following points must be checked:

- Check from the terminal's user web interface, in Menu "Advanced settings > General SIP" that the "Registrar server" parameter is correct.
- check in the configuration files that the parameter "sip registrar ip" is correct.
- Check that the terminal subscription has been created: Menu Subscribers > Subscriptions > Characteristics > General characteristics.
- Check that the SIP service has actually started: Menu System > Configuration > Services.

### 3.44.3 WHY DOESN'T MY MITEL 6000 SIP PHONE RECEIVE THE FTP SERVER IP ADDRESS FROM THE DHCP SERVER?

To assign Mitel 6000 SIP Phone the FTP server IP address to use, the DHCP server must be configured to negotiate with Mitel 6000 SIP Phone:

- either the standard option 66
- or option 43 (vendor specific)



**ATTENTION : If the two options are negotiated at the same time, Mitel 6000 SIP Phone will first take into account Option 43 before Option 66. Option 43 is supported as of version 2.1.2.**

Check that these two options are configured on the DHCP server, and indicate:

- the protocol to use,
- the password associated with the FTP server storage directory,
- FTP server IP address

For a network architecture with several VLANs and/or several subnets, check that the router configuration allows the transmission of the broadcast frames sent by the terminal to the right DHCP server, using the DHCP RELAY information.

# 4 DESCRIPTION OF MIVOICE 5361 DIGITAL PHONE, 5370 DIGITAL PHONE AND 5380 DIGITAL PHONE

The MiVoice 5300 series Digital Phone consists of three terminal types:

- MiVoice 5361 Digital Phone,
- MiVoice 5370 Digital Phone,
- MiVoice 5380 Digital Phone.

MiVoice 5370 Digital Phone and 5380 IP Phone can be used with an extension module.

The proprietary MiVoice 5370 and 5380 Digital Phones are managed as of release R5000.1 R5.1B Phase 2 on Mitel 5000 Gateways and MiVoice 5000 Server.

The proprietary MiVoice 5361 Digital Phone is managed as of release MiVoice 5000 R5.3 on Mitel 5000 Gateways and MiVoice 5000 Server.

The terminal's behaviour is determined by the system (ergonomics, audio, etc.).

**ATTENTION : MiVoice 5300-series Digital Phones are also compatible with the ASCOTEL range. They have the same sales references.**

## 4.1 MIVOICE 5361 DIGITAL PHONE




### 4.1.1 DESCRIPTION OF MIVOICE 5361 DIGITAL PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 4.1.2 SALES CODE FOR MIVOICE 5361 DIGITAL PHONE

The sales code for MiVoice 5361 Digital Phone without mains unit is 20351063.

## 4.2 MIVOICE 5370 DIGITAL PHONE



### 4.2.1 DESCRIPTION OF MIVOICE 5370 DIGITAL PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 4.2.2 SALES CODE FOR MIVOICE 5370 DIGITAL PHONE

The sales code for MiVoice 5370 Digital Phone without mains unit is 20350820.

## 4.3 MIVOICE 5380 DIGITAL PHONE



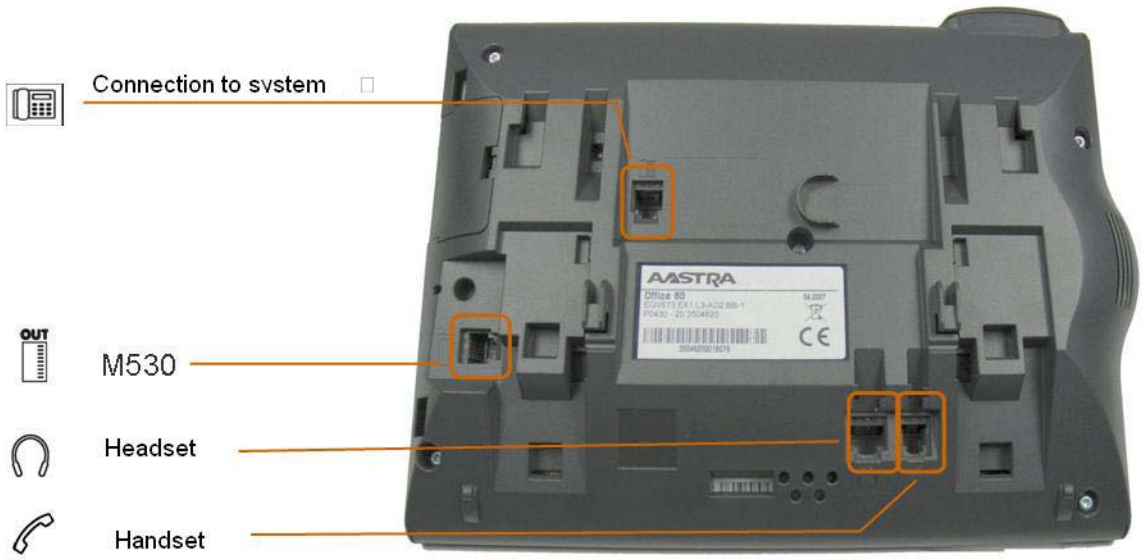
### 4.3.1 DESCRIPTION OF MIVOICE 5380 DIGITAL PHONE

A detailed description of the terminal is given in the user guide (see Section 1.5.1).

### 4.3.2 SALES CODE FOR MIVOICE 5380 DIGITAL PHONE

The sales code for MiVoice 5380 Digital Phone with AZERTY keypad and without mains unit is 20350886. The sales code for MiVoice 5380 Digital Phone with QWERTY keypad and without mains unit is 20350823.

## 4.4 MIVOICE 5300 DIGITAL PHONE CONNECTIONS




### 4.4.1 HEADSETS COMPATIBLE WITH MIVOICE 5370 DIGITAL PHONE AND 5380 IP PHONE

The headset socket for 5370 and 5380 IP Phones is compatible with DHSG standard.

The wiring for the RJ45 headset is as follows:

| Pin | Description |
|---|---|
| 1 | Signalling (from headset to terminal) |
| 2 | 0V (Signal GND) |
| 3 | MIC- |
| 4 | Loudspeaker |
| 5 | Loudspeaker |
| 6 | MIC+ |
| 7 | DC in (3.3 V DC) |
| 8 | Signalling (from terminal to headset) |

Input impedance (MIC-/MIC+):15 k ohms

Output impedance (loudspeaker/loudspeaker): 150 ohms

The following headsets have Mitel price references:

- GN2000 from GN-Netcom: wired headset with sales code AHR0204AA01
- GN9120 from GN-Netcom: wireless headset with sales code AHR0207AA01
- GN9350 from GN-Netcom: wireless headset with DHSG cable and sales code AHR0207AA01

Headsets GN9120 and GN9350 have two operating modes:

- DHSG mode,
- RHL mode.

**ATTENTION : The "automatic off-hook" function offered by the DHSG protocol is only available on MiVoice 5300 IP Phone and MiVoice 5300 Digital Phone.**

Since 5370 and 5380 IP Phones are DHSP-compatible, remote line seizure / on-hook is done

via the headset button or by lifting / placing the headset on its cradle.

RHL mode allows these headsets to be used on other Mitel terminals (6755/6757, M/i740, M/i760, 6753 SIP/55i/57i).

A special cable is obligatory for headsets GN9350 and GN9120 to work in DHSG mode. It comes with headset GN9350.

To configure the operating modes of headsets GN9120 and GN9350, see Chapter 2.5.2

## 4.5 MIVOICE M530 EXTENSION MODULE

An extension module is available and can be used on MiVoice 5370 Digital Phone and 5380 IP Phone.

The sales code for the MiVoice M530 expansion module is 20350804.

| Touches de fonction programmable disponibles | | | |
|---|---|---|---|
| MiVoice 5370 IP Phone | | MiVoice 5380 IP Phone | |
| Terminal | 12 | Terminal | – |
| max. 1M530 | 20 | max. 3M530 | 60 |
| Total | 32 | Total | 60 |

**Note : The "Presence" key is used as an additional programmable key.**

### 4.5.1 CHARACTERISTICS OF THE MIVOICE M530 EXTENSION MODULE

- Direct power supply from the terminal
- 20 programmable keys, with associated LEDs (line, dial, Do not Disturb, etc.)
- Up to 3 modules per terminal:
  - Maximum one module per MiVoice 5370 Digital Phone
  - Maximum three modules per MiVoice 5380 Digital Phone

**Note : The firmware of the extension module is loaded during its first connection to the terminal.**

## 4.6 OPTIONAL ACCESSORIES

The following accessories are available:

- Batch of 10 handset cables for MiVoice 5300 Digital Phone/ MiVoice 5300 IP Phone: AHT0531A
- Batch of 10 stands for MiVoice 5300 Digital Phone/ MiVoice 5300 IP Phone:AHT0532A
- Batch of 10 M530 extension connection cables: AHT0533A
- Batch of 10 stands for M530 extension: AHT0534A

## 4.7 MANAGEMENT OF MIVOICE 5361 DIGITAL PHONE, 5370 DIGITAL PHONE AND 5380 DIGITAL PHONE BY TMA

5361 Digital, 5370 Digital and 5380 Digital phones are managed from TMA:

- Either integrated into Mitel 5000 Gateways, see Section 6.19
- Or hosted by MiVoice 5000 Manager, see Section 7.12.

# 5 TMA - GENERAL INFORMATION (MIVOICE 5000 MANAGER AND INTEGRATED SYSTEM)

## 5.1 GENERAL INFORMATION

The TMA (**T**erminal **M**anagement **A**pplication) is used to deploy and update the following terminals:

- MiVoice 5300 IP phones,
- Mitel 6000 SIP Phones,
- MiVoice 5300 Digital Phones (TDM).

For all the other terminal types, only inventory is possible and only from TMA on  Manager.

TMA may be integrated into a Mitel 5000 Gateways system (accessible from Web Admin) or centralised on a MiVoice 5000 Manager.



**ATTENTION : The integrated TMA service must be deactivated on the different sites when the TMA of MiVoice 5000 Manager is used.**

No special additional licence is required to use TMA. However, the **Subscriber management** licence must be unlocked in tMiVoice 5000 Manager to access the TMA start menu.

The application is generally in charge of providing configuration software and files on one or more FTP servers.

Depending on terminal type, with TMA you can take the following actions:

**MiVoice 5300 IP phones,**

- Deploy MiVoice 5300 IP phones:
  - Deploy MiVoice  5300  IP Phones automatically via the **manual login** function,
  - Deploy the terminals via an Excel form,
- Take an inventory of (logged and unlogged) MiVoice 5300 IP Phones,
- Update the (logged and unlogged) terminal software release:
  - Manage the production release
  - Manage a test release: this function allows a new software release to be loaded only on one part of the terminals so it can be tested before being deployed if necessary on all the terminals in the installation.
- Update the (logged and unlogged) terminal data:
  - Update terminal global data
  - Update specific terminal data

- Export (logged and unlogged) terminal configuration files in .csv format:
  - Export global terminal data
  - Export specific terminal data
- Encrypting the configuration files (specific file only)
- Downloading files directly into FTP server(s) (example: certificate)

**Mitel 6000 SIP Phones**

- Deploy Mitel 6000 SIP Phones:
  - Deploy Mitel 6000 SIP Phones automatically via the **manual login** function,
  - Deploy the terminals via an Excel form,
- Take an inventory of (logged and unlogged) Mitel 6000 SIP Phones,
- Update the (logged and unlogged) terminal software release:
  - Manage the production release
  - Manage a test release: this function allows a new software release to be loaded only on one part of the terminals so it can be tested before being deployed if necessary on all the terminals in the installation.
- Update the (logged and unlogged) terminal data:
  - Update terminal global data
  - Update specific terminal data
- Manage system keys (Template):
  - A **Template** file may be added to the specific data to configure the system keys in addition to those managed from Web Admin.
- Export (logged and unlogged) terminal configuration files in .csv format:
  - Export global terminal data
  - Export specific terminal data
- Encrypting the configuration files (specific and global file)
- Downloading files directly into FTP server(s):
  - A file **modele.cfg** may be downloaded to configure the system keys in addition to those managed from Web Admin.
  - Certificates.
- Activating the Remote worker function: see the document Remote Worker via MBG - AMT/PTD/PBX/0161 - for more information about the deployment of this function.

**Mivoice 5300 Digital Phones (TDM)**

- Take an inventory of the Mivoice 5300 Digital Phones in the installation
- Update the terminal software release:
  - Manage the production release
  - Manage a test release: this function allows a new software release to be loaded only on one part of the terminals so it can be tested before being deployed if necessary on all the terminals in the installation.

**Other terminal types**

- Take an inventory of other terminals on the installation.

## 5.2 MAIN DIFFERENCES BETWEEN TMA ON MIVOICE 5000 MANAGER AND INTEGRATED TMA

### 5.2.1 DIFFERENCES IN TERMS OF DESIGN

The TMA in MiVoice 5000 Manager is used to manage terminals in a multi-site configuration. Therefore, select first for the terminal type concerned:

- The region
- The Multi-site.

The TMA application will then be started with this initialized data.

### 5.2.2 FUNCTIONAL DIFFERENCES

The functional differences are:

- MiVoice 5000 Manager **Server configuration** menu: To create or add a new external storage FTP server and define its configuration parameters, we propose to retrieve the default login/password defined in an integrated TMA context. The accounts defined by default for an integrated server, if appropriate, may be restored automatically by clicking **Initialize embeddedd**.
- **iPBX configuration** menu: this menu is available on MiVoice 5000 Manager only.
  - It is used to send a request to an iPBX in order to delete the TDW tables containing the data version and index information expected for the terminals. This menu must be used after a TMA / TMA-EP passage. This function is only available for sites as of R5.2 SP1.
  - This menu is also used to manage the integrated FTP server, i.e. to delete the content of the FTP areas on an iPBX (as of R6.3). This function can be useful if you wish to use an integrated FTP server in TMA in MiVoice 5000 Manager.
- **Application configuration** menu:

  For MiVoice 5000 Manager, this menu is used to:
  - configure the application management mode (TMA or TMA-EP),
  - temporarily exclude one or more maintenance sites
  - test the configuration (accessible to FTP sites and servers)
- Menu **Terminal configuration export:** The **specific site data** button is used to export in **.csv** format only the specific data of terminals in site-based production software release. This function is used to export the specific data meant to be used by TMA-EP.

### 5.2.3 MENUS AVAILABLE ACCORDING TO TERMINAL RANGE

All the menus can be used for Mitel 6000 SIP Phone and MiVoice 5300 IP Phone.

Only the following menus are applicable for TDM terminals, MiVoice 5300 Digital Phone range:

- Inventory
- Software management
- Actions display
- Events Log

### 5.2.4 COMPARISON OF THE TMA SERVICES AVAILABLE IN MIVOICE 5000 MANAGER AND INTEGRATED INTO MIVOICE 5000

| **TMA services in MiVoice 5000 Manager Multi-site configuration** | **Integrated TMA services in MiVoice 5000 Single-site configuration** |
|---|---|
| Terminal management | |
| Mitel 6000 SIP Phone, MiVoice 5300 IP Phone, MiVoice 5300 Digital phone | Mitel 6000 SIP Phone, MiVoice 5300 IP Phone, MiVoice 5300 Digital phone |
| Terminals logged on and not logged on to the multi-site network | Terminals logged on and not logged on to the site |
| Inventory | |
| All types of terminals | All types of terminals |
| FTP | |
| External | External or integrated |
| Software management | |
| For terminals MiVoice 5300 IP Phone, MiVoice 5300 Digital phone, Mitel 6000 SIP Phone | For terminals MiVoice 5300 IP Phone, MiVoice 5300 Digital phone, Mitel 6000 SIP Phone |
| Manual operation in TMA to trigger terminal software update for:<br>- A list of terminals (test mode)<br>- All the terminals (production mode) | Manual operation in TMA to trigger terminal software update for:<br>- A list of terminals (test mode)<br>- All the terminals (production mode) |
| | Automatic terminal software update when the integrated FTP server is used. |
| Configuring terminals MiVoice 5300 IP Phone et Mitel 6000 SIP Phone | |
| Manual operation in TMA to trigger terminal configuration update for:<br>- A list of terminals (test mode)<br>- All the terminals (production mode) | Manual operation in TMA to trigger terminal configuration update for:<br>- A list of terminals (test mode)<br>- All the terminals (production mode) |
| Configuration file export | Configuration file export |
| | Automatic update of the terminal's global configuration file when the integrated FTP server is used. |
| Configuring terminals Mitel 6000 SIP Phone | |
| A file **modele.cfg** can be directly downloaded into the FTP servers. | A file **modele.cfg** can be directly downloaded into the FTP servers. |

**ATTENTION : For the functions available in TMA-EP mode, see the TMA-EP operating manual (AMT/PTD/TR/0027*).**

# 6 MANAGING TERMINALS WITH THE TMA INTEGRATED INTO MIVOICE 5000

**TMA**: (**T**erminal **M**anagement **A**pplication)

TMA may be integrated either into a Mitel 5000 Gateways system or MiVoice 5000 Server (accessible from Web Admin) or centralised on a MiVoice 5000 Manager.

This chapter is devoted to the integrated TMA application. For management from MiVoice 5000 Manager, see Chapter 7).

The integrated TMA is accessible via the Terminal Service menu, on the Web Admin welcome screen.

## 6.1 PRESENTATION AND PRINCIPLES

TMA, integrated into MiVoice 5000 Manager and MiVoice 5000 Server, is used to deploy and manage the following terminals:

- Proprietary MiVoice 5300 IP phones,
- Mitel 6000 SIP Phones
- Mivoice 5300 Digital Phones (TDM)

The main actions on the terminals, based on the range, are described in Chapter 5.

The TMA integrated into Mitel 5000 Gateways and MiVoice 5000 Server systems has a single-site range only.

No specific additional software licence is required to use the integrated TMA application. However, the licences for SIP and IP subscribers must be unlocked.

The integrated TMA is compatible with the FTP server integrated into Mitel 5000 Gateways and MiVoice 5000 Server, as well as with external FTP servers; the principles are respectively:

- **For an integrated FTP server**, the integrated TMA application creates some symbolic links between the directories on the FTP server and the tree directories of the TMA application.



**Note : If the configuration file encryption function is enabled, the encrypted configuration files are physically copied into the integrated FTP server storage directories.**

- **For an external FTP server**, the integrated TMA application uses some FTP accounts to copy the files (configuration software and files) from the TMA application directories to the external FTP server storage directories.



**Note : During each terminal update operation (software, configuration), TMA checks the accessibility of the sites and external FTP servers concerned by the action. In case of error during this check, the action is not performed.**

## 6.2 LAUNCHING THE TMA APPLICATION

From Web Admin, start the TMA application by selecting **Terminal Service**:

The **Terminal service** is activated while first installing and upgrading.

If the **Terminal service** is not activated, in Web Admin, select Menu **Telephony service > System > Configuration > Services** and start the **TERMINAL service**.

- The TMA welcome window opens.

The following menus are accessible in the left column:

- **Call Dist**: This menu is used to return to the Web Admin home page.
- **Application configuration**: This menu is used to activate or not the management of the selected models.
  - Desactive the management of global and specific data files and to retain only software update actions on the terminals, in the actions managed by TMA
  - Activate the configuration file encryption mode
  - Activatie the Remote worker function: see the document Remote Worker via MBG - AMT/PTD/PBX/0161 - for more information about the deployment of this function.
- **Model management**: This menu is used to activate or not the model management
- **Servers configuration**: This menu is used to define the parameters of the external storage FTP server(s).
- **Inventory**: This menu is used to view the inventory of installation terminals and manage the list of terminals.
- **Software management**: This menu is used to install and manage the terminal software releases and start terminal update actions.
- **Terminals configuration**: This menu is used to distribute the global and specific parameters and to start data update on the terminal.
- **Deployment**: this menu is used to deploy the terminals manually.
  This menu is also used to make available to the FTP server(s) the template files (modele.cfg) used by Mitel 6000 SIP Phones and the certificates (ca.crt) used by Mitel 6000 SIP Phones and MiVoice 5300 IP Phones.
- **Terminals configuration export**: This menu is used to export in **.csv** format the global and specific data about Mitel 6000 SIP Phones and MiVoice 5300 IP Phones.
- **Actions display**: This menu is used to display the actions started on the terminals (deployment, terminal software, global and specific data).
- **Events log**: This menu displays the events log.

# 6.3 CONFIGURING TMA

## 6.3.1 CONFIGURING THE TERMINALS

For Mitel 6000 SIP Phones and MiVoice 5300 IP Phones, TMA is dedicated to the management of two data types:

- The software release compared to that of the iPBX
- The global and specific data about each terminal model, depending on the range in question.

In some cases, only the management of software release may be necessary on these two terminal ranges.

The **Application configuration** menu can be used to disable the management of configuration files and, thus, to also disable the deployment actions and to only preserve the terminal software update operations.

The following operations will not be carried out:

- Automatic terminal software and global data updates if the iPBX is upgraded (if the integrated FTP server integrated into the Mitel 5000 Gateways or MiVoice 5000 Server is started),
- Automatic global data configuration file update
- Taking into account the templates for Mitel 6000 SIP Phones,
- Encrypting configuration files

Select the **Application configuration** menu from the TMA main menu.

- Untick the **Terminals configuration** box.
- Click **Validate**.
- Only terminal software update menus will then be proposed.

## 6.3.2 ENCRYPTING CONFIGURATION FILES

The **Application configuration** menu is also used to activate the configuration file encryption function:

- For MiVoice 5300 IP Phones, only specific configuration files are encrypted.
- For Mitel 6000 SIP Phones, the specific and global configuration files, as well as the template files modele.cfg made available via the deployment menu are encrypted.

The configuration files of MiVoice 5300 IP Phones are encrypted automatically by TMA during the following operations:

- Specific data update
- Deployment via the Excel form

The configuration files of Mitel 6000 SIP Phones are encrypted automatically by TMA during the following operations:

- Specific data update
- Global data update
- Deployment via the Excel form
- Terminal software package update in production mode and test mode

- Automatic terminal software and global data updates if the iPBX is upgraded (if the integrated FTP server integrated into the Mitel 5000 Gateways or MiVoice 5000 Server is started),
- Automatic update of the global data configuration file after certain parameters are modified via Web Admin (terminal VLAN, PC VLAN, LLDP, etc.),
- Taking some templates into account for Mitel 6000 SIP Phones when the terminal is first registered.

To activate configuration file encryption, select the **Application configuration** menu from the TMA main menu.

- Tick the **Configuration file encryption** checkbox.
- Click **Validate**.
- Validate the confirmation message by clicking **Yes**.

**ATTENTION : Configuration file encryption can only be deactivated manually. Contact Mitel technical support.**

## 6.4 MODEL MANAGEMENT

Model management is carried out from this menu and is taken into account in the Embedded TMA.

When downloading a terminal package, Embedded TMA retains only software of the managed model s.

As a result, during a software update, only the files related to the managed models are sent to the FTP servers.

## 6.5 FTP SERVER CONFIGURATION PARAMETERS

### 6.5.1 INTRODUCTION

TMA is generally in charge of providing some configuration software and files on one or more FTP servers during day-to-day terminal deployment or management.

- **Single-site configuration**

  For Mitel 5000 Gateways and a single-site configuration, an integrated FTP server is available and is automatically configured during the automatic start procedure in STANDARD or TOTAL mode using **CTRL + i**, or when it is started manually via Web Admin.

**Note : The integrated FTP server of the TMA integrated into Mitel 5000 Gateways is automatically configured and accessible from the Server configuration menu.**

For MiVoice 5000 Server and a single-site configuration, an integrated FTP server is available and is automatically configured during the automatic start procedure in STANDARD or TOTAL mode using CTRL + i, or when it is started manually via Web Admin.

**ATTENTION : For MiVoice 5000 Server, the FTP service must first be installed during the start procedure in STANDARD or TOTAL mode using CTRL + i. The FTP service can then be started automatically or manually via Web Admin.**

Providing configuration software and files:

- **For an integrated FTP server**, the integrated TMA application creates some symbolic links between the storage directories on the FTP server and the work directories of TMA.

**Note : If the configuration file encryption function is enabled, the encrypted configuration files are physically copied into the integrated FTP server storage directories.**

- **For an external FTP server**, the integrated TMA application uses some FTP accounts to copy the files (configuration software and files) from the TMA work directories to the storage directories of the external FTP server.

**Note : In R5.3 and later, during each terminal update operation (terminal software, configuration files), TMA checks the accessibility of the sites and external FTP servers concerned by the action. In case of error during this check, the action is not performed.**

- **Multi-site configuration**

  In this case, TMA is started from MiVoice 5000 Manager and the FTP servers must be manually defined in the **Servers configuration** menu.

  Follow the procedure described in Section 7.6.4.2.3 - Configuring external FTP server(s).

  The FTP servers integrated into the multi-site Mitel 5000 Gateways and MiVoice 5000 Server may be used by identifying and configuring them from MiVoice 5000 Manager in the same **Servers configuration** menu.

## 6.5.2 USING THE FTP SERVER INTEGRATED INTO MITEL 5000 GATEWAYS AND MIVOICE 5000 SERVER.

### *6.5.2.1 Starting the FTP service on Mitel 5000 Gateways*

By default, the integrated FTP server is installed and started when the Mitel 5000 Gateways system is installed. To check its status, proceed as follows:

From the web browser, connect to the system's MiVoice 5000 Web Admin.

Go to the service management menu:

- this menu (231) is accessible via **Telephony Service** >**System > Configuration > Services**

Check the status of the **FTP service** which must be **STARTED**. Otherwise, it must be started manually through this menu or automatically through the procedure described in Chapter 6.7.5.

### *6.5.2.2 Starting the FTP service on MiVoice 5000 Server*

By default, the integrated FTP server is not **installed** and started when MiVoice 5000 Server is installed. Therefore, the **FTP service** is not visible in Menu **Telephony service** >**System > Configuration > Services** (231). For the installation and configuration of the integrated FTP server on MiVoice 5000 Server while starting in STANDARD or TOTAL mode using **CTRL + i**, refer to Sections 6.10.4 and 6.10.5.

### *6.5.2.3 Configuring the start of the integrated FTP server on Mitel 5000 Gateways*

For automatic configuration of the starting of the integrated FTP server on Mitel 5000 Gateways while starting in STANDARD or TOTAL mode using **CTRL + i**, refer to Section 6.7.5.

#### 6.5.2.4 *Automatic configuration of integrated FTP server accounts for MiVoice 5300 IP Phones.*

The accounts are configured and managed automatically as follows on Mitel 5000 Gateways and MiVoice 5000 systems:

The following accounts are created by default for MiVoice 5300 IP Phones:

| DEDICATED DIRECTORIES * | RIGHT | LOGIN | PASSWORD |
|---|---|---|---|
| /opt/a5000/infra/sip_sets/53xxip<br>Production release | Read/Write via FTP | mngt_ftp_53xxip | mngt_ftp_53xxip |
| /opt/a5000/infra/sip_sets/53xxip<br>Production release | Reading via FTP | aamadeus | aamadeus |
| /opt/a5000/infra/sip_sets/test_53xxip<br>Test version | Read/Write via FTP | mngt_test_53xxip | mngt_test_53xxip |
| /opt/a5000/infra/sip_sets/test_53xxip<br>Test version | Reading via FTP | test_aamadeus | test_aamadeus |

#### 6.5.2.5 *Automatic configuration of integrated FTP server accounts for Mitel 6000 SIP Phone*

The accounts are configured and managed automatically as follows on Mitel 5000 Gateways and MiVoice 5000 systems:

The following accounts are created by default for **Mitel 6000 SIP Phones**:

| DEDICATED DIRECTORIES * | RIGHT | LOGIN | PASSWORD |
|---|---|---|---|
| /opt/a5000/infra/sip_sets/deploy-ment_67xxi<br>Production release for deployment | Reading via FTP | connexio | connexio |
| /opt/a5000/infra/sip_sets/67xxi<br>Production release | Read/Write via FTP | mngt_ftp_67xxi | mngt_ftp_67xxi |
| /opt/a5000/infra/sip_sets/67xxi<br>Test version | Reading via FTP | ftp_67xxi | ftp_67xxi |
| /opt/a5000/infra/sip_sets/test_67xxi<br>Test version | Reading via FTP | test_connexio | test_connexio |
| /opt/a5000/infra/sip_sets/test_67xxi<br>Test version | Read/Write via FTP | mngt_test_67xxi | mngt_test_67xxi |
| /opt/a5000/infra/sip_sets/pictures<br>Pictures of 6739 SIP, 6867 SIP, 6869 SIP and 6873 SIP phones | Reading via FTP | picture | picture |
| /opt/a5000/infra/sip_sets/blustar<br>Blustar 8000i | Read/Write via FTP | blustar | blustar |



**Note : For information about how to manage pictures on 6739 SIP, 6867 SIP, 6869 SIP and 6873 SIP phones, see the document AMT/PTD/PBX/0114*.**



**Note : For information on how to manage pictures on Blustar 8000i, see document AMT/PTD/TLA/0063*.**

#### 6.5.2.6 Constraints concerning the use of the integrated FTP server on Mitel 5000 Gateways

The integrated FTP server on Mitel 5000 Gateways, due to its combination with ToIP applications, is limited as regards the number of simultaneous connections. The duration of terminal update is about 2 minutes. The terminal is not available during this period.

The limitations are as follows:

- The limit in terms of number of simultaneous transfers is **30** for terminals Mitel 6000 SIP Phones.
- The limit in terms of number of simultaneous transfers is **60** for MiVoice 5300 IP Phones.

#### 6.5.2.7 Constraints concerning the use of the integrated FTP server on MiVoice 5000 Server

The limitations are as follows:

- The limit in terms of number of simultaneous transfers is **1000** for **Mitel 6000 SIP Phones** and MiVoice 5300 IP Phones.

#### 6.5.2.8 Configuring external FTP server accounts manually in TMA for Mitel 6000 SIP Phones and MiVoice 5300 IP phones .

In the other cases, the external FTP server(s) is/are configured manually from the **Servers configuration** menu:

- Click **Add new server**.
- Fill in the different fields and confirm.

All the accounts must be created manually by referring, for instance, to those defined in Sections 6.5.2.4 and 6.5.2.4 .

#### 6.5.2.9 Configuring accounts on the external FTP server

See Chapter 11 to create the same storage directory access accounts and password as those defined in integrated TMA, in the previous chapter.

# 6.6 DHCP SERVER CONFIGURATION PARAMETERS

## 6.6.1 INTRODUCTION

The DHCP server is used to automatically assign an IP address to Mitel 6000 SIP Phone and MiVoice 5300 IP Phone, with a lease, and to negotiate some standard and specific network parameters with them. These parameters will enable them to download the terminal software and configuration files placed in the right storage areas on the FTP server in question.

The parameters which can be negotiated with Mitel 6000 SIP Phone and MiVoice 5300 IP Phone are described in Chapters 9 and 10.

The type of DHCP server used depends on the type of configuration.

- **Single-site configuration**

  For Mitel 5000 Gateways and MiVoice 5000 Server, as well as a single-site configuration, an integrated DHCP server is available and configurable:

  - Either automatically during the start procedure in STANDARD or TOTAL mode using **CTRL + i**. This method is highly recommended in this type of configuration.
  - Either manually from the Web Admin **DHCP SERVICE** menu. Refer to Chapter 9 .

- **Multi-site configuration**

  In this case, the DHCP server is external and must be configured manually. See Chapter 10 for more information about external DHCP server configuration.

## 6.6.2 STARTING THE INTEGRATED DHCP SERVICE ON MITEL 5000 GATEWAYS

The integrated DHCP server on Mitel 5000 Gateways is not started by default when the Mitel 5000 Gateways system is installed.

To see its status, proceed as follows:

From the web browser, connect to the system's MiVoice 5000 Web Admin.

Go to the service management menu:

- this menu (231) is accessible via **Telephony Service** >**System > Configuration > Services.**

Check the status of the **DHCP service** which must be **STOPPED**. It may be started manually through this menu or started and configured automatically through the procedure described in Chapter 6.7.5 .

## 6.6.3 STARTING THE INTEGRATED DHCP SERVICE ON MIVOICE 5000 SERVER

By default, the integrated DHCP server on MiVoice 5000 Server is not installed and started when MiVoice 5000 Server is installed. Therefore, the **DHCP service** is not accessible in Menu **Telephony service** >**System > Configuration > Services** (231). For the installation and configuration of the start of the integrated DHCP server on MiVoice 5000 Server while starting in STANDARD or TOTAL mode using **CTRL + i**, refer to Sections 6.10.4 and 6.10.5.

# 6.7 DEPLOYING THE TERMINALS FOR A NEW MITEL 5000 GATEWAYS INSTALLATION

## 6.7.1 PRINCIPLE

The advantage of using integrated TMA in the deployment phase lies in the possibility to automate the deployment of IP terminals using the integrated TMA, FTP and DHCP services. This automatic configuration is made during the start procedure in STANDARD or TOTAL mode using **CTRL + i**.

**Note : See also the document Mitel 5000 Gateways and MiVoice 5000 Server - Implementation - AMT/PTD/PBX/0151* for more information about start-up and installation.**

## 6.7.2 CONFIGURING THE SYSTEM VIA CTRL I

Access is provided locally on the COM port of the CPU card, using a NULL MODEM cable (ref.: BHG0024A) connected between the COM port of the CPU card and the PC COM port.

On the PC connected to the COM port

- Open a Hyperterminal window and configure the connection as follows:
  - Bits per second: 115200 b/s
  - Data bits: 10/8
  - Parity: "none"
  - Stop bits: 10/1
  - Flow control: None
- Power on the system and follow the start-up progress on the PC.
- Upon display of "**Identification starting**"
- Press **Ctrl** + **I:** the screen then displays the different configuration modes.

```
*-------------------------------------------------*
| Configuration mode (F/T/S/P/U/E) : S            |
| - F : Factory mode                              |
| - T : Total mode                                |
| - S : Standard mode                             |
| - P : Password reset                            |
| - U : USB provisionning mode                    |
| - E : for Exit                                  |
*-------------------------------------------------*
```

- Select "**p**" mode then press "**Enter**" to enter the network parameters configuration menu.

### 6.7.3 CONFIGURING NETWORK PARAMETERS IN MITEL 5000 GATEWAYS

- The system's default network configuration is displayed on screen.

```
*-------------------------------------------------*
| ENTER IP ADDRESS :     192.168.65.1             |
| ENTER NETWORK MASK :   255.255.255.0            |
| ENTER GATEWAY :        192.168.65.254           |
| ENTER DNS1 :                                    |
| ENTER DNS2:                                     |
*-------------------------------------------------*
Do you want to change configuration Y/[N] : Y
```

- Press "**Y**" then "**Enter**" to access the different fields.
- Enter successively the system parameters, using the **Enter** key to change line.

```
*-------------------------------------------------*
| ENTER IP ADDRESS :     20.1.1.2                 |
| ENTER NETWORK MASK :   255.255.255.0            |
| ENTER GATEWAY :        20.1.1.254               |
| ENTER DNS1 :                                    |
| ENTER DNS2:                                     |
```

- After the last line is validated, a summary of the network parameters is displayed for confirmation.

```
*-------------------------------------------------*
| RESUME                                          |
*-------------------------------------------------*
*-------------------------------------------------*
| IPADR =              20.1.1.2                   |
| NETWORKMASK =        255.255.255.0              |
| GATEWAY =            20.1.1.254                 |
| DNS1 :                                          |
| DNS2:                                           |
| NETWORKADDR =        20.1.1.0                   |
| BROADCAST =          20.1.1.255                 |
*-------------------------------------------------*
Do you confirm (Y/N) ? Y
```

- Press "**Y**" to confirm the input or "**N**", in case or error, to enter the network parameters again.

### 6.7.4 CONFIGURING FLOW SEPARATION IN MITEL 5000 GATEWAYS

The screen then displays the flow separation configuration for signals and data.

**ATTENTION : Answer "N" and go to the next screen. If necessary, refer to the flow separation operating manual (AMT/PTD/PBX/0101*).**

```
*-----------------------------------------------------------
| DO YOU WANT TO CONFIGURE MANAGEMENT IP NETWORK ? [Y]/N : N
*-----------------------------------------------------------
_*
```

### 6.7.5 CONFIGURING THE INTEGRATED SERVICES IN MITEL 5000 GATEWAYS WHILE STARTING THE SYSTEM

The screen below is used to define the status of the integrated services when starting the system, so as to automate terminal deployment.

By default, the TMA and FTP services are started automatically (TMA = 1, FTP = 1). The integrated DHCP server must also be started and configured automatically.

**Note : These services can also be activated later from Web Admin if automatic deployment is not envisaged.**

```
An existing configuration was found
*-------------------------------------------------*
| FTP : 1                                         |
| TMA : 1                                         |
| DHCP : 0                                        |
*-------------------------------------------------*
```

- Press "**Y**" to modify the configuration and set automatic start of the integrated DHCP server.

```
*-------------------------------------------------*
| FTP : 1                                         |
| TMA : 1                                         |
| DHCP: 1                                         |
*-------------------------------------------------*
Do you confirm (Y/N) ? Y
```

- Press "**Y**" to confirm the input.

## 6.7.6 DEFINING THE PARAMETERS FOR AUTOMATIC DEPLOYMENT OF MITEL 6000 SIP PHONES IN MITEL 5000 GATEWAYS

The screen below is used to define the parameters for automatically deploying Mitel 6000 SIP phones.

```
*-------------------------------------------------*
| Configuration mode (F/T/S/P/U/E) : S            |
| - F : Factory mode                              |
| - T : Total mode                                |
| - S : Standard mode                             |
| - P : Password reset                            |
| - U : USB provisionning mode                    |
| - E : for Exit                                  |
*-------------------------------------------------*
```

- Press "**N**". Press "**Y**" to modify the default configuration, if necessary.

The default parameters are as follows:

- LLDP ENABLED=**0**
  - This field is used to activate the LLDP protocol in the terminal, (1 = yes) or no (0= no).

**Note : This value can also be viewed and modified via the Web Admin menu Telephony service > Subscribers > Terminals and Applications > 6xxxi parameters.**

### *6.7.6.1 LLDP functions of 6735 SIP, 6737 SIP, 6863 SIP, 6865 SIP, 6867 SIP, 6869 SIP and 6873 SIP phones (optional):*

Mitel 6735 SIP Phone, 6737 SIP, 6863 SIP, 6865 SIP, 6867 SIP, 6869 SIP and 6873 SIP phones are compatible with LLDP-MED in order to acquire the VLAN number (Vlan ID) with which they must work. This operating mode is active by default on the terminals and, to be operational, the terminals must be connected to a network SWITCH compatible with this function. This latter must then provide the required VLAN ID.

However, when a terminal is started, a first DHCP DISCOVER request may be sent without VLAN tag (default VLAN of the SWITCH), or in the data VLAN if already configured in the terminal.

The acquisition of an IP address in this default VLAN is not mandatory, and the DHCP request sent may remain without any reply.

If an IP address is assigned to the terminal by a DHCP server, it is immediately released through a DHCP RELEASE before a new DHCP DISCOVER request is made in the new VLAN acquired during the LLDP discover procedure.

Thereafter, the terminal continues to work in the VLAN sent by the SWITCH with an IP address assigned by a DHCP server in the corresponding IP subnet.

### 6.7.7 DEFINING THE PARAMETERS OF THE INTEGRATED DHCP SERVER IN MITEL 5000 GATEWAYS

The screen below is used to define the configuration parameters of the integrated DHCP server in Mitel 5000 Gateways. This menu is used to define the parameters that allow the integrated DHCP server to be configured automatically for MiVoice 5300 IP phone, Mitel 6000 SIP Phone and i7xx.

**Note : Manual configuration of the DHCP server is available from Web Admin and allows the modification of the automatic configuration defined via this menu. See Chapter 9 for more information on how to manually configure the DHCP server.**

```
 *-------------------------------------------------*
| SUBNET MASK :                                    |
| BEGIN RANGE :                                    |
| END RANGE :                                      |
| GATEWAY :                                        |
| VLAN POSTE:                                      |
| VLAN PC :                                        |
*-------------------------------------------------*
Please_enter_valid_IP_BEGINRANGE
```

- Enter successively the configuration parameters of the integrated DHCP server, using the **Enter** key to change line.
  - **SUBNET MASK**: Subnet mask for MiVoice 5300 IP phone, Mitel 6000 SIP Phone and i7xx.
  - **BEGIN RANGE and END RANGE**: Address range for MiVoice 5300 IP phone, Mitel 6000 SIP Phone and i7xx.
  - **GATEWAY**: Gateway IP address of the network reserved for MiVoice 5300 IP Phone, Mitel 6000 SIP phone and i7xx.
  - **TERMINAL VLAN and PC VLAN**: These parameters are used to define the LAN port and PC port VLAN dedicated to Mitel 6000 SIP Phones, MiVoice 5300 IP Phone and i7xx. They are not mandatory for simple networks (do not make any entry on the line concerned and press **Enter)**.

```
 *-------------------------------------------------*
| SUBNET MASK :     255.255.255.0                  |
| BEGIN RANGE :     20.1.1.100                     |
| END RANGE :       20.1.1.199                     |
| GATEWAY :         20.1.1.254                     |
| VLAN POSTE:                                      |
| VLAN PC :                                        |
*-------------------------------------------------*
Do you confirm (Y)/(N) ? Y
```

Answer "**Y**" to the question:

```
Do you want to apply your change Y(es)/N(o)/R(econfigure) ?
```

The procedure for configuring the system via **CTRL I** has ended and the system restarts.

### 6.7.8 RESTARTING MITEL 5000 GATEWAYS

After the system is restarted, the automatic configuration phase last about 5 minutes.

During this period, the following main actions are taken:

- The DHCP server integrated to manage MiVoice 5300 IP Phone and Mitel 6000 SIP Phone (as well as i7xx) is automatically configured.
- The new network parameters of the integrated FTP server are taken into account in the integrated TMA application.
- The global data configuration file used to deploy Mitel 6000 SIP Phones is updated with the information entered previously using **CTRL I.**

**Note : In factory presetting, the global data configuration file used to deploy Mitel 6000 SIP Phones is automatically updated with the country-location and operation information.**

- The index of the global data configuration file of Mitel 6000 SIP Phones, which can be used by the integrated TMA, is updated. An action is automatically started by the integrated TMA to update the system data (the index of the global data configuration file used for deployment and by TMA remains identical. This prevents, after the first manual login of the Mitel 6000 SIP Phone, a terminal update request by the system).

**Note : In factory presetting:**

- **The production software release of the integrated TMA is automatically configured with the software releases of Mitel 6000 SIP Phones and MiVoice 5300 IP Phones, contained in MiVoice 5000 R6.2.**
- **The software releases of the Mitel 6000 SIP Phones and MiVoice 5300 IP Phones contained in MiVoice 5000 R6.2 are moved to the work directory of the integrated TMA (as of R5.4 SP1, some symbolic links are available in the directory deployment_67xxi: these symbolic links point to the TMA work directory or are stored in the software release of the production Mitel 6000 SIP Phone. There is no change for the global deployment configuration file aastra.cfg which remains physically present in this location).**
- **Some automatic actions are automatically started by the integrated TMA to update the software releases and global data configuration file of MiVoice 5300 IP Phone and Mitel 6000 SIP Phone (respectively files localdb.config.ftp and aastra.cfg).**

Automatic terminal configuration is enabled by default, as well as automatic update of the numbering plan and Mitel 6000 SIP Phone system keys, management of programmable keys, languages and pictures of Mitel 6000 SIP Phones (Menu Telephony service > Subscribers > Terminals and Applications > 6xxxi parameters).

The checks to be made before deploying MiVoice 5300 IP Phones and Mitel 6000 SIP Phones are indicated in the following sections.

To access the configuration menus of the integrated TMA, click the **Terminal service** menu from the Web Admin portal.

### 6.7.9 CHECKING THE CONFIGURATION OF THE INTEGRATED DHCP SERVER ON MITEL 5000 GATEWAYS:

The **network** dedicated to MiVoice 5300 IP Phones, Mitel 6000 SIP Phones and i7xx is automatically configured using **CTRL + I**:

All models of the terminals associated with these three terminal ranges can be configured for the **network.** The **network** is also automatically configured with the information entered **CTRL I**:

- Subnet name
- Sub-network address
- Subnet mask
- IP address range
- Lease duration
- Router IP address.

For each terminal range concerned, the DHCP options are equally configured automatically using the information entered with **CTRL I**:

- Integrated FTP server IP address
- Main PBX IP address...

### 6.7.10 CHECKING THE CONFIGURATION OF THE INTEGRATED FTP SERVER IN MITEL 5000 GATEWAYS

The storage directories used for daily management and deployment of MiVoice 5300 IP phones, Mitel 6000 SIP phones and Mivoice 5300 Digital phones are automatically created in the Mitel 5000 Gateways. The main directory under which these directories are located is called **opt/a5000/infra/sip_sets**.

Each storage directory is accessible via an account (login/password) which defines the possible actions according to user type and terminal type.

The configuration of the integrated FTP server used by the integrated TMA is automatically defined and can be viewed in the **Servers configuration** menu (Action: **Modify**).

**Note : The fields Login/Write password and Login/Test Write password are not filled in because the integrated TMA uses some symbolic links to provide, in the right storage folders, the configuration software and files used by MiVoice 5300 IP Phone, Mitel 6000 SIP Phone and MiVoice 5300 Digital Phone.**

See Chapters 6.5.2.4 and 6.5.2.5 for the definition of the accounts used by MiVoice 5300 IP Phone and Mitel 6000 SIP Phone.

**For MiVoice 5300 Digital Phones:**

The created directory is empty; it will be loaded later during update operations.

### 6.7.11 CHECKING THE CONFIGURATION OF THE PRODUCTION SOFTWARE RELEASE OF MIVOICE 5300 IP PHONES AND MITEL 6000 SIP PHONES

The production terminal software release is automatically defined after the factory pre-configuration made in the integrated TMA and in the Mitel 5000 Gateways data. The **Software management** menu is used to check the production terminal software release for each terminal range.

The information is displayed in the **Production software release** field.

## 6.8 DEPLOYING MITEL 6000 SIP PHONES ON A NEW MITEL 5000 GATEWAYS INSTALLATION

**Note : As from release R5.1C, Mitel 6000 SIP Phones can be managed from the integrated TMA.**

It is possible to log on Mitel 6000 SIP Phone via the MiVoice 5000 User Portal application. A new global 6xxxi parameter is used to open this feature. The user selects a terminal on which to log on via the MiVoice 5000 User Portal application from its system label. For each terminal, this label is unique and automatically generated by the Mitel 5000 Gateways system. This label can be modified individually or massively.

A global parameter can be configured to disable the free seating function. In this case (parameter unticked, the impact is as follows:

- On Mitel 6000 SIP Phone terminals, the Ident key is no longer displayed, and manual login from the terminals is rejected for all the Mitel 6000 SIP Phones on the installation.

This parameter is accessible via Menu **Telephony service** > **Subscribers** > **Terminals and Applications** > **6xxxi parameters**, and is called **Manual login authorisation on any terminal type**. By default, this parameter is enabled (ticked). This parameter is accessible if login via MiVoice 5000 User Portal is open.

A new tool for deploying Mitel 6000 SIP Phones through automatic login is configurable by automatically assigning a directory number to each terminal identified by its unique label. Automatic login is carried out next time the terminal is registered. This tool concerns all the (secure and unsecured) subscriptions.

It is possible to secure or not the login tool during the Mitel 6000 SIP Phone deployment phase. A new subscription parameter is used to carry out this configuration:

- In non-secure mode, the parameter **Login via PC only** is not ticked (default value): the user can log on manually via the Ident key or via the corresponding feature code (*44 by default).
- In secure mode, the parameter **Login via PC only** is ticked: the user cannot log on manually via the Ident key or via the corresponding feature code (*44 by default).

As of R6.2, it is possible to reinforce the security of the MiVoice 5000 User Portal access by configuring and using Single Sign-on (SSO) mode (see document AMT/PTD/PBX/0080* for how to configure SSO mode).

After the pre-configuration made in Chapter 6.6, Mitel 6000 SIP Phones can be deployed using the following methods:

- Deployment through manual login on the terminal (**as of R5.2 only)**
- Deployment via MiVoice 5000 User Portal from a unique label identifying the terminal (**as of R6.2 only)**
- Automatic deployment by assigning a subscription number to the terminal (**as of R6.2 only)**
- Deployment from a dedicated Excel file

## 6.8.1 DEPLOYING MITEL 6000 SIP PHONES THROUGH MANUAL LOGIN

### *6.8.1.1 Principle*

This deployment method consists in making a manual login on Mitel 6000 SIP Phones without having to indicate the specific configuration file **@MAC.cfg,**. The production software release and global data configuration file downloaded by Mitel 6000 SIP Phones during this deployment phase are available in the storage folder **deployment_67xxi**. This folder is accessible to Mitel 6000 SIP Phones via the account connexio/connexio, the default factory account of Mitel 6000 SIP Phone.

### *6.8.1.2 Procedure*

Prerequisites:

- The subscription of the Mitel 6000 SIP Phone on which manual login must be performed must be declared in the Mitel 5000 Gateways.
- A directory record must exist for this subscription.
- Log in via PC should not be enabled:
  - In the Web Admin menu **Telephony service** > **Subscriptions** > **Terminals and Applications** > **6xxxi parameters**, the parameter **Login via PC** should not be ticked (default value).



**ATTENTION : It is advisable to restore the factory configuration before any deployment operation via manual login.**

Procedure:

- Connect the terminal to the network in question.
- The terminal is initialised and connects to the integrated DHCP server. The integrated DHCP server will then assign an IP address to the terminal. The integrated DHCP server will also provide Mitel 6000 SIP Phone with the IP address of the integrated FTP server and the account (connexio/connexio) to which Mitel 6000 SIP Phone will connect to download its production software release and global deployment data configuration file.
- After the new production software release and global configuration file are downloaded, the terminal screen shows that the terminal is a general-purpose terminal (without subscriber).
- Press the **Ident** key which lights up by default (key 4).
- Enter the subscription number of Mitel 6000 SIP Phone then confirm by pressing **Enter**.
- Enter the subscription password (**0000** by default) and press **Enter** or **OK** to confirm.
- A wait message appears and the terminal logs on to its subscription.
- The terminal is operational; the idle screen is displayed.

## 6.8.2 DEPLOYING MITEL 6000 SIP PHONES VIA MIVOICE 5000 USER PORTAL

### *6.8.2.1 Principle*

The principle of this deployment method is to log on via the MiVoice 5000 User Portal. The user selects a terminal on which to log on from its system label. This label is unique and automatically generated by the Mitel 5000 Gateways system.

**Note : The user can log on to the MiVoice 5000 User Portal application via his specific User Portal password or in SSO mode.**

### *6.8.2.2 Procedure*

Prerequisites:

- The subscription of the Mitel 6000 SIP Phone on which manual login must be performed must be declared in the Mitel 5000 Gateways.
- A directory record must exist for this subscription.
- Log in via PC must be enabled:
  - In the Web Admin menu **Telephony service** > **Subscriptions** > **Terminals and Applications** > **6xxxi parameters**, the parameter **Login via PC** must be ticked.
- A default label must be configured.
  - In the Web Admin menu **Telephony service** > **Subscribers** > **Terminals and Applications** > **6xxxi parameters**, the parameter **Label format** must be defined (an example of label is indicated from the defined format).
  - This default label can be configured:
    - individually in the Web Admin menu **Telephony service** > **Subscribers** > **Terminals and Applications** > **Terminal label management,**
    - massively by exporting/importing all the labels in .csv format.

**ATTENTION : It is advisable to restore the terminal's factory settings before any deployment operation.**

Procedure:

- Connect the terminal to the network in question.
- The terminal is initialised and connects to the integrated DHCP server. The integrated DHCP server will then assign an IP address to the terminal. The integrated DHCP server will also provide Mitel 6000 SIP Phone with the IP address of the integrated FTP server and the account (connexio/connexio) to which Mitel 6000 SIP Phone will connect to download its production software release and global deployment data configuration file.
- After the new production software release and global configuration file are downloaded, the terminal screen shows the label defined for this terminal.

**Note : Since it is set to non-secure mode, the user can also log on manually and directly to his terminal using the Ident key.**

- Connect to MiVoice 5000 User Portal (in SSO mode or via the directly via the directory number and User Portal password).
- Select Menu **Terminals** > **Login/Logout.**
- Select a free terminal and its label, either by selecting a terminal available in the log or by entering a

new terminal.

- Click **Login**.
- The terminal logs on to its subscription.
- The terminal is operational; the idle screen is displayed.

## 6.8.3 DEPLOYING MITEL 6000 SIP PHONES AUTOMATICALLY

### *6.8.3.1 Principle*

The principle of this deployment method is to carry out an automatic login of Mitel 6000 SIP Phones by automatically assigning a directory number to each terminal identified by its unique label.

### *6.8.3.2 Procedure*

Prerequisites:

- The subscription of the Mitel 6000 SIP Phones on which automatic login must be performed must be declared in the Mitel 5000 Gateways.
- A directory record must exist for this subscription.
- Log in via PC must be enabled:
  - In the Web Admin menu **Telephony service** > **Subscriptions** > **Terminals and Applications** > **6xxxi parameters**, the parameter **Login via PC** must be ticked.
- A default label must be configured.
  - In the Web Admin menu **Telephony service** > **Subscribers** > **Terminals and Applications** > **6xxxi parameters**, the parameter **Label format** must be defined (an example of label is indicated from the defined format).
  - This default label can be configured:
    - individually in the Web Admin menu **Telephony service** > **Subscribers** > **Terminals and Applications** > **Terminal label management,**
    - massively by exporting/importing all the labels in .csv format.
- The directory number must be assigned to a each label:
    - individually in the Web Admin menu **Telephony service** > **Subscribers** > **Terminals and Applications** > **Terminal label management,**
    - massively by exporting/importing all the labels in .csv format.



**ATTENTION : It is advisable to restore the terminal's factory settings before any deployment operation.**

Procedure:

- Connect the terminal to the network in question.
- The terminal is initialised and connects to the integrated DHCP server. The integrated DHCP server will then assign an IP address to the terminal. The integrated DHCP server will also provide Mitel 6000 SIP Phone with the IP address of the integrated FTP server and the account (connexio/connexio) to which Mitel 6000 SIP Phone will connect to download its production software release and global deployment data configuration file.
- After the new production software release and global configuration file are downloaded, the terminal screen shows the label defined for this terminal.

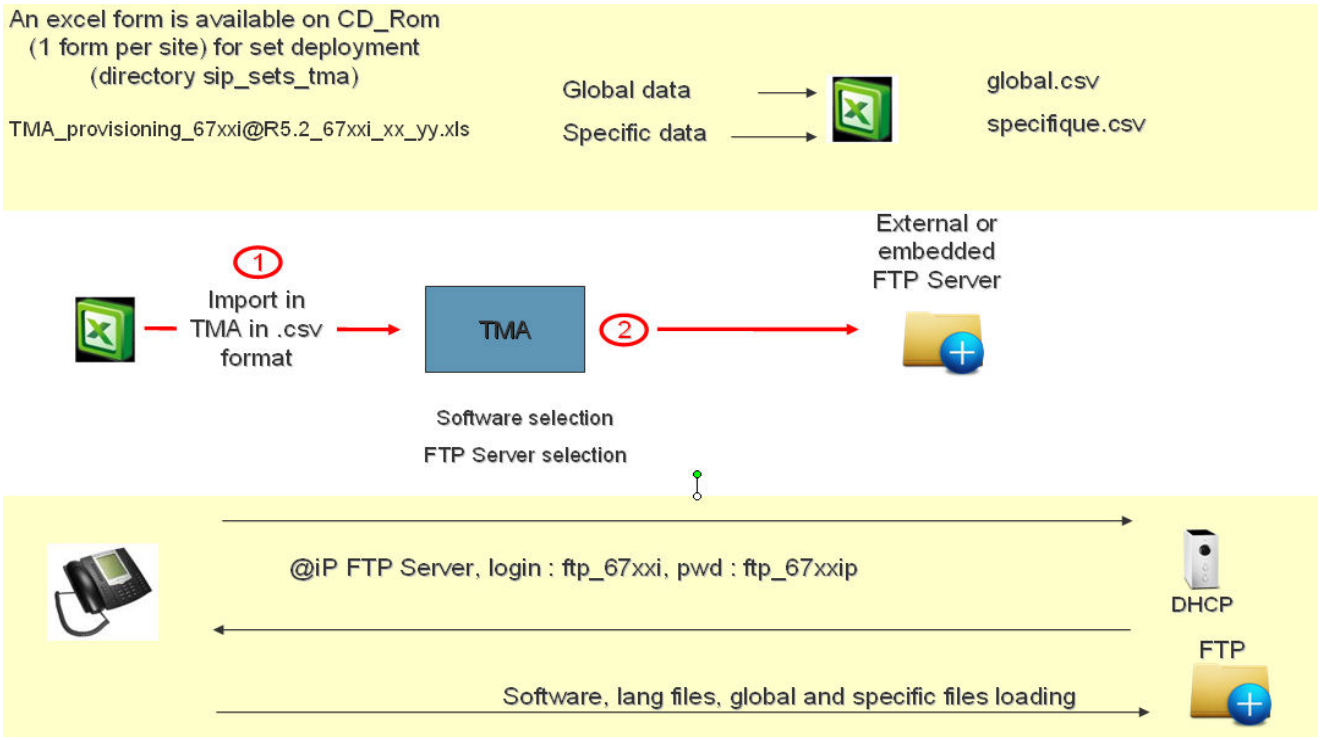
- The terminal logs on automatically to its subscription.
- The terminal is operational; the idle screen is displayed.

## 6.8.4 DEPLOYING MITEL 6000 SIP PHONES THROUGH AN EXCEL FORM

### *6.8.4.1 Principle*

This method consists in deploying the terminals via an Excel form provided with the MiVoice 5000 R6.2 software CDROM dedicated to the deployment of terminals Mitel 6000 SIP Phones. This method requires modifying the DHCP server configuration so Mitel 6000 SIP Phone connects to the account used for day-to-day management (default ftp_67xxi on an integrated FTP server).

The diagram below illustrates this method.




- A form is provided with the MiVoice 5000 R6.2 software CDROM. From this form, the terminals' global and specific data is collected and exported in .csv format. Specific data is indexed by terminal MAC address.

**Note : After the configuration performed previously with CTRL I, the integrated FTP server is configured automatically.**

**Note : The terminal software package R6.2 was installed automatically and defined as production release, after the configuration performed previously with CTRL I.**

- The operator selects:
  - The global and specific data of Mitel 6000 SIP Phones in .csv format to be imported into TMA
  - The terminal software to be deployed
  - Eventually other files such as template files **modele.cfg** or a certificate..
  - The integrated FTP server on which this data must be stored.
- The operator validates the deployment operation: the terminal software, language files, global and specific data are then automatically sent to the integrated FTP server via some symbolic links.

- The operator connects the terminal to the local area network and this latter registers to its reference site via automatic login using the login site optimisation mechanism if necessary.

### *6.8.4.2 Procedure*

#### 6.8.4.2.1 Collecting global and specific data via the Excel form

The Excel form **TMA_provisionning_67xxi@R6.2_67xxi_xx_yy.xls** is available on the MiVoice 5000 R6.2 software CD-ROM, in the directory **sip_sets_tma**.

The Excel form contains the following tabs:

- The **Import_CSV_TMA** tab used only with the TMA EP application, refer to the document AMT/PTD/TR/0027 .
- The **67xxi Global** tab in which the global data of Mitel 6000 SIP Phones is defined
- The **67xxi Specific** tab in which the specific data of Mitel 6000 SIP Phones is defined
- The **67xxi All** tab in which all the parameters used by Mitel 6000 SIP Phones are defined.
- The **68xxi_Teleworker** tab used for the remote worker feature, refer to the document AMT/PTD/PBX/0161/.

All or part of the parameters in the **67xxi All** tab may or may not be managed in the global or specific data, depending on the required distribution of the parameters.

To add a parameter in the **67xxi Global** tab, copy from the **67xxi All** the parameter concerned, located in the **#KEY** column then paste it on the first free line of the **67xxi Global** tab.

To add a parameter in the **67xxi Specific** tab, copy from the **67xxi All** the parameter concerned, located in the **#KEY** column then paste it on the first free column of the **67xxi Specific** tab.

After data distribution, you can collect and export data in .csv format.

#### 6.8.4.2.2 Saving the global and specific data in .csv format

- To save the global data in .csv format:
  - Go to the **67xxi Global** tab.
  - Click the menu **File** > **Save As...**.
  - Go to the right directory, enter a file name then select Type of file **CSV (separator: semicolon) (*.csv)**.
  - Click **Save**.
  - Confirm the next two information messages by clicking **OK** then **YES**.
- To save the specific data in .csv format:
  - Go to the **67xxi Specific** tab.
  - Click the menu **File** > **Save As...**.
  - Go to the right directory, enter a file name then select Type of file **CSV (separator: semicolon) (*.csv)**.
  - Click **Save**.
  - Confirm the next two information messages by clicking **OK** then **YES**.
- Close the Excel form.



**ATTENTION : Never modify the content of .csv files directly. The modifications must be made in the Excel form then saved in .csv format.**

#### 6.8.4.2.3 Deploying the terminal software release and configuration files on the Integrated FTP server

To deploy the terminal software release, language files and configuration files for the global and specific data of Mitel 6000 SIP Phones on the integrated FTP server, proceed as follows.

- From the integrated TMA, click the **Deployment** menu.
- Select the **6xxxi** range.
- In the **List of FTP servers** column, click the integrated FTP server on which the terminal software release and configuration files will be placed.

**Note : If only one FTP server is defined, this will be selected by default.**

- Select the **Software version** to be deployed.

**Note : If only one software release is installed, it will be selected by default.**

- Select the **Global (csv) file** to be deployed:
  - Click **Browse** then select the .csv file to import and which corresponds to the global data of Mitel 6000 SIP Phone from the collection. Click **Open.**
- Select the **Specific (csv) file** to be deployed:
  - Click **Browse** then select the .csv file to import and which corresponds to the specific data of Mitel 6000 SIP Phones from the collection. Click **Open.**
- Il It is also possible to download other files like certificates, templates files (model.cfg) via the field Other file (template, certificate, ...). These downloaded files are kept locally and can be downloaded via the Downloaded Files field.
- Click **Validate** to start deploying the terminal software release and the configuration files of Mitel 6000 SIP Phones: a message indicates that the deployment has been implemented.
- The following files are then placed automatically by TMA in the storage directory of the integrated FTP server by creating symbolic links:
  - The terminal software releases <**such as poste>.st** (example:  55i.st)
  - The global data file **aastra.cfg**
  - The specific data files @MAC.cfg (example: 00085D3A2451.cfg)
  - The language pack files: **lang_<ISO 639>_<ISO 3166>.txt** or **lang_<ISO 639>.txt** (example: lang_fr_ca.txt or lang_de.txt)

**Note : The global and specific data is automatically changed to a format that is compatible with Mitel 6000 SIP Phones by TMA.**

  - The terminals' global and specific data files are also copied automatically to the integrated TMA work directories. This prevents the global and specific data from being entered twice in TMA for day-to-day management of these terminals.

#### 6.8.4.2.4 Checking that the deployment process is working correctly

This operation is used to ensure that the deployment operation has been performed correctly.

- Click the **Action monitoring** menu.
- Check in **Action monitoring,** the status of the deployment operation:
  - If the deployment operation was successful, the status indicates: **Success**
- Check in the **Event log,** the status of the deployment operation:
  - If the deployment operation was successful, the status indicates: **Action successful. Action on MiVoice 5000 PBX taken into account.**
  - The number of transferred files is used to ensure that all the files have actually been placed in the integrated FTP server storage directory.

#### 6.8.4.2.5 Modifying the integrated DHCP server configuration before deployment

This modification is used to temporarily define, during this deployment phase, the account which Mitel 6000 SIP Phones must use to connect to the storage directory in which all the files have just been placed (account ftp_67xxi:ftp_67xxi).

- From the Web Admin home page, click the **DHCP service** menu.
- Click the **DHCP - Operation** menu.
- Click the icon to modify the subnet in question (**network** by default). The subnet parameters definition page opens.
- For **Mitel 6000 SIP Phone**s, modify the login/password **connexio:connexio** through **ftp_67xxi:ftp_67xxi**.
- This modification may also be made based on terminal model.
- Save the new configuration by clicking **Validate**.
- From the global parameters edition page, click **Generate**.
- Validate or do not validate immediate registration of the new configuration. In case of immediate registration: an information message then gives the status of the DHCP status: **The DHCP service is started.**
- Otherwise, click when necessary the menu **Restart DHCP server** to generate the new file dhcpd.conf and restart the DHCP service. An information message then gives the status of the DHCP status: **The DHCP service is started.**

#### 6.8.4.2.6 Connecting the terminals to the local area network

- The operator connects the terminal to the local area network:
  - The terminal retrieves from the DHCP server the IP address of the integrated FTP server with the account to which it must connect.
  - The terminal connects to the integrated FTP server and updates its software release if necessary. The terminal also retrieves its global and specific data configuration files.
  - The terminal registers automatically to its reference site from the information contained in its global and specific data configuration files and is then visible in the TMA inventory.

#### 6.8.4.2.7 Modifying the integrated DHCP server configuration after deployment

After the deployment phase, this modification is used to reset the login/password **connexio:connexio** defined by default in the integrated DHCP server for deployment through deployment login or manual login of Mitel 6000 SIP Phones.

See Chapter 6.7.3.2.5 to configure the login/password **connexio:connexio**.

### 6.8.5 MULTI-COMPANY CONFIGURATION

For a multi-company configuration, if the subscription on which Mitel 6000 SIP Phone is deployed is not in company 0, authorise the EAS user to access the terminal's company.

If an attempt is made to deploy a Mitel 6000 SIP Phone on a subscription that does not belong to company 0 and the action is rejected with the message: **PBX subscription not declared,** proceed as follows:

- Authorise deployment on the company associated with the subscription:
  - Open the menu "External applic.server users" (4.4.7 in a single-site configuration).
  - Click the digit in the number column, which corresponds to the EAS user called **saesae** (generally 1).
  - Tick the box authorising access to the company associated with the subscription.

### 6.8.6 INVENTORY OF MITEL 6000 SIP PHONES

After the deployment of Mitel 6000 SIP Phones, it is necessary to check that they are visible in the integrated TMA inventory, with a software release corresponding to the production software release defined in the integrated TMA.

**Note : The inventory lists all the terminals on the installation.**

The **Inventory** menu is used to check the software release of Mitel 6000 SIP phones after the deployment operation. Logged and unlogged terminals are listed.

- Click the **Inventory** menu.
- Select the **67xxi range** and possibly the **model**.
- Information about each terminal saved on its reference site is displayed.
  - The terminals associated with a production software release appear in green in the **Software version** column.
  - The terminals associated with a test software release appear in orange in the **Software version** column.
  - The terminals associated with any other software release appear in red in the **Software version** column.
  - Information display depends on the filter used. This filter is activated by clicking the icon.
- If possible, apply a filter to the current inventory based on:
  - The terminal subscription number
  - The terminal IP address
  - The terminal software release (production, test release, etc.)
  - The terminal global data index
  - The terminal specific data index
  - The terminal MAC address

- Terminal encryption configuration:
  - SRTP (and TLS) mode activated
  - TLS mode activated
  - No encryption activated

**Note : The joker * may be applied to the parameters Number, IP address and Mac address by placing them at the end of the parameter value.**

- Click**Filter** to apply the filter to the current inventory.

The version of the terminals in the **Software release** column is green in colour if it is the same as the terminal software release defined as the production software release.

The **logged** column is used to indicate whether Mitel 6000 SIP Phone is registered on its reference site (green tick) or whether the terminal is not registered on its reference site (red cross).

The **Periodic logout** column indicates whether Mitel 6000 SIP Phone may or may not log out periodically.

If the terminal is not registered on its reference site, a tooltip indicates the possible reason why the registration failed or whether the terminal is a general-purpose one.

The **Security** column indicates the encryption status of Mitel 6000 SIP Phones:

- Encrypted terminal in SRTP (and TLS): 
- Encrypted terminal in TLS 
- Terminal not encrypted: Empty
- Information not available: 

(configuration file not present or encryption parameters not found)

## 6.9 DEPLOYING MIVOICE 5300 IP PHONES ON A NEW MITEL 5000 GATEWAYS INSTALLATION

A global parameter can be configured to disable the free seating function. In this case (parameter unticked, the impact is as follows:

- On Mitel 5300 SIP Phones, the Ident key remains displayed, but manual login from the terminals is rejected for all the Mitel 5300 SIP Phones on the installation.

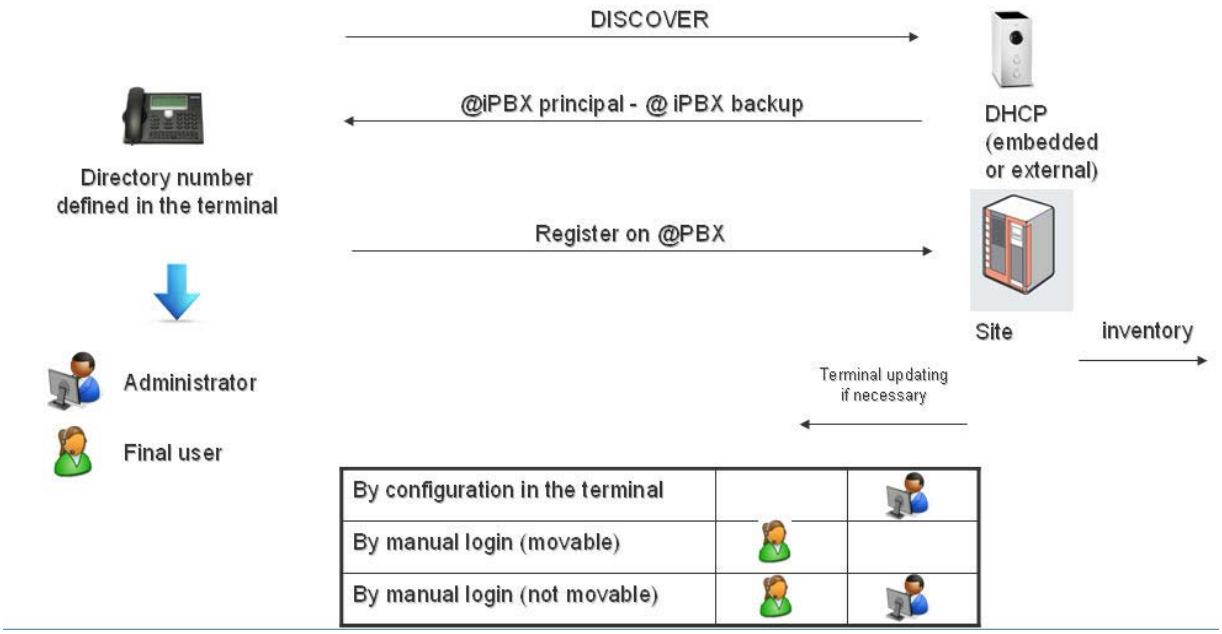
This parameter is accessible via Menu **Telephony service** > **Subscribers** > **Terminals and Applications** > **6xxxi parameters**, and is called **Manual login authorisation on any terminal type**. By default, this parameter is enabled (ticked). This parameter is accessible if login via MiVoice 5000 User Portal is open.

After the pre-configuration made in Chapter 6.6, MiVoice 5300 IP Phones can be deployed using the following two methods:

- Automatic deployment through manual login
- Deployment from an Excel form

### 6.9.1 DEPLOYING MIVOICE 5300 IP PHONES AUTOMATICALLY THROUGH MANUAL LOGIN

#### *6.9.1.1 Principle*




**Note : The administrator may equally configure the directory number manually on the terminal before connecting the terminal to the local area network.**

This deployment method consists in making a manual login on MiVoice 5300 IP Phones without having to indicate the specific configuration file **localdb.config.@MAC.ftp,** unlike the other deployment methods. The production software release and global data configuration file downloaded by MiVoice 5300 IP phones during this deployment phase are available in the MiVoice 5300 IP Phone storage folder. This folder is accessible to MiVoice 5300 IP phones via the aamadeus/aamadeus account, the default factory account of MiVoice 5300 IP Phone.

#### 6.9.1.2 Procedure

Prerequisites:

- The subscription of the MiVoice 5300 IP Phone on which manual login must be performed must be declared in the Mitel 5000 Gateways.
- The free seating function must be enabled.



**ATTENTION : It is advisable to restore the factory configuration before any deployment operation via manual login.**

Procedure:

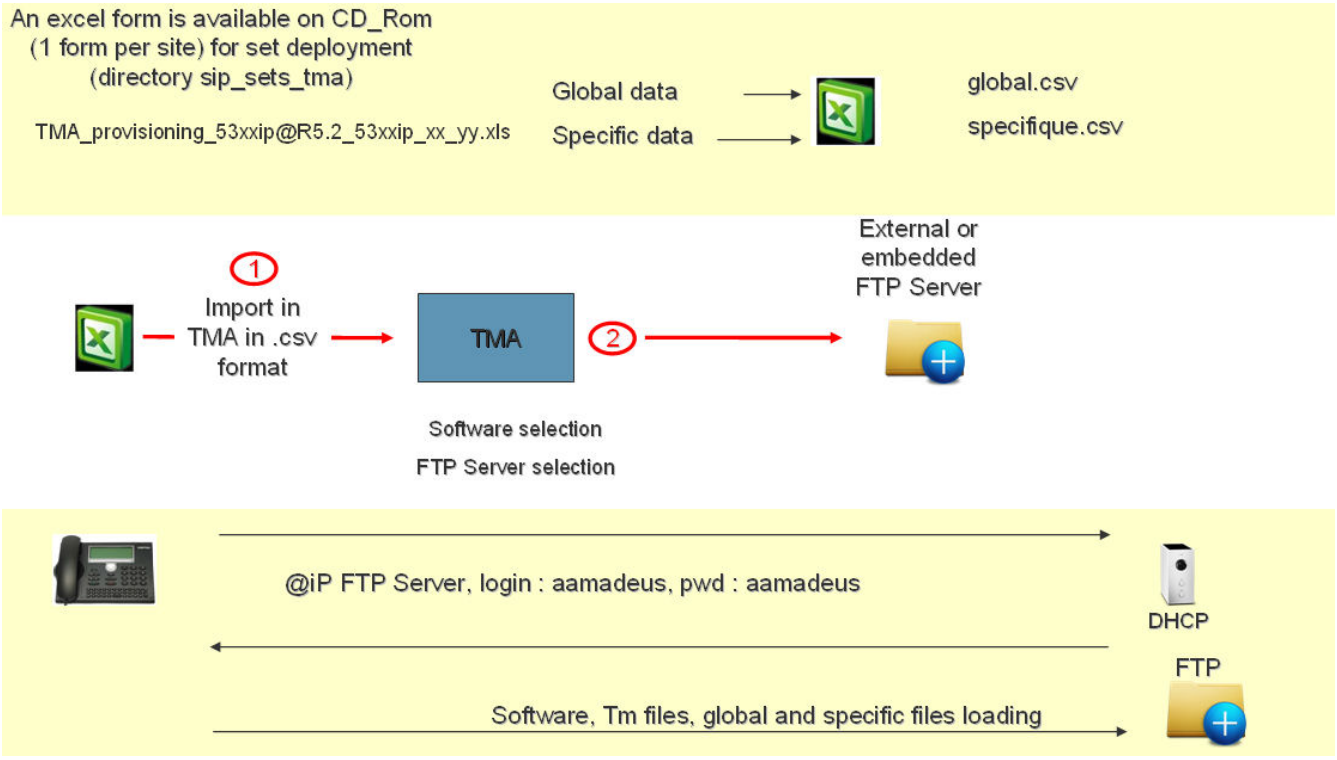
- Connect the terminal to the network in question.
- The terminal is initialised and connects to the integrated DHCP server. The integrated DHCP server will then assign an IP address to the terminal. The integrated DHCP server will also provide MiVoice 5300 IP Phone with the IP address of the integrated FTP server to which MiVoice 5300 IP Phone will connect to download its production software release and global data configuration file. The DHCP server also provides MiVoice 5300 IP Phone with the IP address of the system to which the terminal must log on.
- The terminal screen then proposes identification **Ident**.
- Select **Ident** using the navigation bar.
- Then enter the subscription number of MiVoice 5300 IP Phone and click **OK** to confirm.
- Enter the subscription password (**0000** by default) and press **OK** to confirm.
- The terminal is operational; the idle screen is displayed.

## 6.9.2 DEPLOYING MIVOICE 5300 IP PHONES THROUGH AN EXCEL FORM

### *6.9.2.1 Principle*

This method consists in deploying the terminals via an Excel form provided with the MiVoice 5000 R6.2 software CDROM dedicated to the deployment of terminals MiVoice 5300 IP Phones.

The diagram below illustrates this method.




- A form is provided with the MiVoice 5000 R6.2 software CDROM. From this form, the terminals' global and specific data is collected and exported in .csv format. The specific data is indexed by the terminal MAC address or by the directory number of MiVoice 5300 IP Phone.

**Note : After the configuration performed previously with CTRL I, the integrated FTP server is configured automatically.**

**Note : The terminal software package R6.2 was installed automatically and defined as production release, after the configuration performed previously with CTRL I.**

- The operator selects:
  - The global and specific data of MiVoice 5300 IP Phones in .csv format to be imported into TMA
  - The terminal software to be deployed
  - The integrated FTP server on which this data must be stored.
- The operator validates the deployment operation: the terminal software, Tm files, global and specific data are then automatically sent to the integrated FTP server via some symbolic links.

- The operator connects the terminal to the local area network and this latter registers to its reference site via automatic login using the login site optimisation mechanism if necessary.

**ATTENTION : If the specific files are indexed by the directory number of MiVoice 5300 IP Phones, it is obligatory after the deployment phase to manually delete these files in the storage area of the integrated FTP server.**

### *6.9.2.2 Procedure*

#### 6.9.2.2.1 Collecting global and specific data via the Excel form

The Excel form **TMA_provisionning_53xxip@R6.2_53xxip_xx_yy.xls** is available on the MiVoice 5000 R6.1 software CD-ROM, in the directory **sip_sets_tma**.

The Excel form contains three tabs:

- The **Global** tab in which the global data of MiVoice 5300 IP Phones is defined
- The **Specific** tab in which the specific data of MiVoice 5300 IP Phones is defined
- The **Other** tab in which all the parameters used by MiVoice 5300 IP Phones are defined.

All or part of the parameters in the **Other** tab may or may not be managed in the global or specific data, depending on the required distribution of the parameters.

To add a parameter in the **Global** or **Specific** tab, copy from the **Other** tab the parameter concerned, located in the **KEY** column then paste it on the first free column of the **Global** or **Specific** tab.

If you wish to make a deployment with some specific data indexed by directory number, the **MAC_ADDRESS** column of the **Specific** tab should not be filled in.

Data collection can be made once the data is distributed.

**ATTENTION : The DNS_NAME parameter must be available and its value must be empty.**

#### 6.9.2.2.2 Saving the global and specific data in .csv format

- To save the global data in .csv format:
  - Go to the **Global** tab.
  - Click the menu **File** > **Save As...**.
  - Go to the right directory, enter a file name then select Type of file **CSV (separator: semicolon) (*.csv)**.
  - Click **Save**.
  - Confirm the next two information messages by clicking **OK** then **YES**.
- To save the specific data in .csv format:
  - Go to the **Specific** tab.
  - Click the menu **File** > **Save As...**.
  - Go to the right directory, enter a file name then select Type of file **CSV (separator: semicolon) (*.csv)**.
  - Click **Save**.

- Confirm the next two information messages by clicking **OK** then **YES**.

- Close the Excel form.



**ATTENTION : Never modify the content of .csv files directly. The modifications must be made in the Excel form then saved in .csv format.**

#### 6.9.2.2.3 Deploying the terminal software release and configuration files on the Integrated FTP server

To deploy the terminal software and configuration files for the terminals' global and specific data on the integrated FTP server, proceed as follows:

- Click the **Deployment** menu.
- Select the **53xxip** range.
- In the **List of FTP servers** column, click the integrated FTP server on which the terminal software release and configuration files will be placed.



**Note : If only one FTP server is defined, this will be selected by default.**

- Select the **Software version** to be deployed.



**Note : If only one software release is installed, it will be selected by default.**

- Select the **Global (csv) file** to be deployed:
  - Click **Browse** then select the .csv file to import and which corresponds to the global data of MiVoice 5300 IP Phones from the collection. Click **Open.**
- Select the **Specific (csv) file** to be deployed:
  - Click **Browse** then select the .csv file to import and which corresponds to the specific data of MiVoice 5300 IP Phones from the collection. Click **Open.**
- Click **Validate** to start deploying the terminal software release and the configuration files of MiVoice 5300 IP Phones: a message indicates that the deployment has been implemented.
- The following files are then placed automatically by TMA in the storage directory of the integrated FTP server by creating symbolic links:
  - The terminal software release (aamxip_<vn>.ftp, tm.config.<tt>.<vn>.ftp)
  - The global data file (localdb.config.ftp)
  - The specific data files (localdb.config.<mac>.ftp ou localdb.config.<NA>.ftp)



**Note : The global and specific data is automatically changed to a format that is compatible with MiVoice 5300 IP Phones by TMA.**

- The terminals' global and specific data files are also copied automatically to the integrated TMA work directories. This prevents the global and specific data from being entered twice in TMA for day-to-day management of these terminals.

#### 6.9.2.2.4 Checking that the deployment process is working correctly

This operation is used to ensure that the deployment operation has been performed correctly.

- Click the **Action monitoring** menu.
- Check in **Action monitoring,** the status of the deployment operation:
  - If the deployment operation was successful, the status indicates: **Success**
- Check in the **Event log,** the status of the deployment operation:
  - If the deployment operation was successful, the status indicates: **Action successful. Action on MiVoice 5000 PBX taken into account.**
  - The number of transferred files is used to ensure that all the files have actually been placed in the integrated FTP server storage directory.

#### 6.9.2.2.5 Connecting the terminals to the local area network

- The operator connects the terminal to the local area network by first entering its directory number if the specific data is indexed by the directory number:
  - The terminal retrieves the IP address of the integrated FTP server from the DHCP server.
  - The terminal connects to the integrated FTP server and updates its software release if necessary. The terminal also retrieves its global and specific data configuration files.
  - The terminal registers automatically to its reference site from the information contained in its global and specific data configuration files and is then visible in the TMA inventory.

### 6.9.3 INVENTORY OF MIVOICE 5300 IP PHONES

After the deployment of MiVoice 5300 IP Phones, it is necessary to check that they are visible in the integrated TMA inventory, with a software release corresponding to the production software release defined in the integrated TMA.

**Note : The inventory lists all the terminals on the installation.**

The **Inventory** menu is used to check the software release of MiVoice 5300 IP Phones after the deployment operation. Logged and unlogged terminals are listed.

- Click the **Inventory** menu.
- Select the **53xxip range** and possibly the **model**.
- Information about each terminal saved on its reference site is displayed.
  - The terminals associated with a production software release appear in green in the **Software version** column.
  - The terminals associated with a test software release appear in orange in the **Software version** column.
  - The terminals associated with any other software release appear in red in the **Software version** column.
  - Information display depends on the filter used. This filter is activated by clicking the icon. 
- If possible, apply a filter to the current inventory based on:
  - The terminal subscription number
  - The terminal IP address
  - The terminal software release (production, test release, etc.)
  - The terminal global data index

- The terminal specific data index
- The terminal MAC address
- Terminal encryption configuration:
  - SRTP (and TLS) mode activated
  - No encryption activated

**Note : The joker * may be applied to the parameters Number, IP address and Mac address by placing them at the end of the parameter value.**

- Click**Filter** to apply the filter to the current inventory.

  The version of the terminals in the **Software release** column is green in colour if it is the same as the terminal software release defined as the production software release.

  The **logged** column is used to indicate whether MiVoice 5300 IP Phone is registered on its reference site (green tick) or whether the terminal is not registered on its reference site (red cross).

  If the terminal is not registered on its reference site, a tooltip indicates the possible reason why the registration failed or whether the terminal is a general-purpose one.

  The **Security** column indicates the encryption status of MiVoice 5300 IP Phones:

- Encrypted terminal in SRTP (and TLS): 
- Terminal not encrypted: Empty
- Information not available: 

  (configuration file not present or encryption parameters not found)

# 6.10 DEPLOYING TERMINALS ON A NEW MIVOICE 5000 SERVER INSTALLATION

## 6.10.1 PRINCIPLE

**For MiVoice 5000 server**, the TMA, FTP and DHCP services are available and managed via Web Admin to simplify terminal deployment. The FTP and DHCP services must first be installed while starting the MiVoice 5000 Server in STANDARD or TOTAL RECONFIGURE mode before being managed via Web Admin.

**ATTENTION : A service should only be installed if it is not used by the client for its own needs, especially the DHCP service. An installed service cannot be uninstalled.**

**Note : In general, MiVoice 5000 Server is integrated into a multi-site architecture and associated with the MiVoice 5000 Manager in which the FTP and DHCP services are external.**

**Note : See also the document Mitel 5000 Gateways and MiVoice 5000 Server - Implementation - AMT/PTD/PBX/0151* for more information about implementing an installation.**

## 6.10.2 CONFIGURING THE SYSTEM VIA CTRL I

It is possible to configure the telephony network IP address by double-clicking the **Standard reconfigure** shortcut, available on the MiVoice 5000 Server PC desktop.

**Note : For a redundant MiVoice 5000 Server configuration, the Standard Reconfigure shortcut must be started from the active MiVoice 5000 Server PC.**

```
*-------------------------------------------------------------------------*
| Select the IP you want to enable for the                                |
| A5000 server (Telephony Network side)                                   |
| Enter the choice number or another IP address                           |
| 0 : 20.1.1.1                                                            |
| 1 : Another                                                             |
*-------------------------------------------------------------------------*

Enter your choice : [20.1.1.1] ?
You choose 20.1.1.1, do you confirm [Y]/N ? y
```

- If necessary, change the telephony network IP address.
- Confirm the input by typing in **Y**.

### 6.10.3 CONFIGURING FLOW SEPARATION IN MIVOICE 5000 SERVER

The screen then displays the flow separation configuration for signals and data.



**ATTENTION : Answer "N" and go to the next screen. If necessary, refer to the flow separation operating manual (AMT/PTD/PBX/0101*).**

### 6.10.4 INSTALLING THE INTEGRATED SERVICES ON MIVOICE 5000 SERVER

```
*-------------------------------------------------------------
| DO YOU WANT TO CONFIGURE MANAGEMENT IP NETWORK ? [Y]/N : N
*-------------------------------------------------------------*
```

This screen is used to install the integrated services on MiVoice 5000 Server which must be managed by Web Admin. By default, only the TFTP, ANNOUNCEMENT and IVR services are installed.



**Note : For a redundant MiVoice 5000Server, the DHCP service cannot be installed and managed via Web Admin. As of R6.2, the integrated DHCP service is available in a redundant MiVoice 5000 Server configuration.**

```
ACTUAL CONFIGURATION IS :
*-------------------------------------------------------------------------
-----*
| DHCP (0/1) :                0                                          |
| FTP (0/1) :                 0                                          |
| TFTP (0/1) :                1                                          |
| SYSLOG (0/1) :              0                                          |
| SSH (0/1) :                 0                                          |
| ANNOUNCEMENT (0/1) :        1                                          |
| IVR (0/1) :                 1                                          |
| IVB (0/1) :                 0                                          |
| CONFERENCE (0/1) :          1                                          |
*-------------------------------------------------------------------------*
DO YOU WANT TO CHANGE CONFIGURATION Y/[N] ? Y
```

Type in "Y" to modify the configuration and configure the installation of the DHCP, FTP and Syslog services.

.

```
ACTUAL CONFIGURATION IS :
*-------------------------------------------------------------------------
-----*
| DHCP (0/1) :                1                                          |
| FTP (0/1) :                 1                                          |
| TFTP (0/1) :                1                                          |
| SYSLOG (0/1) :              1                                          |
| SSH (0/1) :                 0                                          |
| ANNOUNCEMENT (0/1) :        1                                          |
| IVR (0/1) :                 1                                          |
| IVB (0/1) :                 0                                          |
| CONFERENCE (0/1) :          1                                          |
*-------------------------------------------------------------------------*
Do you confirm (Y/N) Press enter to reconfigure ? Y
```

Press "Y" to confirm the input.

### 6.10.5 AUTOMATIC START OF THE INTEGRATED SERVICES ON MIVOICE 5000 SERVER

The screen below is used to define the status of the integrated services during start-up.

By default, the TMA service is started automatically.

**Note : These services can also be started later from Web Admin.**

```
An existing configuration was found
*-------------------------------------------------*
| FTP : 0|
| TMA : 1|
| DHCP : 0                                        |
*-------------------------------------------------*
DO YOU WANT TO CHANGE CONFIGURATION Y(ES)/N(O)  ? Y
```

- Press "Y" to modify the configuration and set automatic start of the integrated FTP and DHCP services.

```
 *-------------------------------------------------*
 | FTP : 1                                         |
 | TMA : 1                                         |
 | DHCP : 1                                        |
 *-------------------------------------------------*
Do you confirm (Y/N) Press enter to reconfigure? Y
```

- Press "Y" to confirm the input.

### 6.10.6 DEFINING THE PARAMETERS FOR AUTOMATIC DEPLOYMENT OF MITEL 6000 SIP PHONES IN MIVOICE 5000 SERVER

The screen below is used to define the parameters for automatically deploying Mitel 6000 SIP phones.

```
An existing configuration was found
*-------------------------------------------------*
| LLDP ENABLED : 0                                |
*-------------------------------------------------*
Do you want to change configuration Y(es)/N(o)  ?  N
```

- Press "N". Press "Y" to modify the default configuration, if necessary.

See Chapter 6.7.6 for details and meaning of the parameters.

### 6.10.7 AUTOMATIC CONFIGURATION OF THE INTEGRATED DHCP SERVER PARAMETERS ON MIVOICE 5000 SERVER

The screen below is used to define the configuration parameters of the integrated DHCP server in MiVoice 5000 Server. This menu is used to define the parameters that allow the integrated DHCP server to be configured automatically for MiVoice 5300 IP phone, Mitel 6000 SIP Phone and i7xx.

**Note : Manual configuration of the DHCP server is available from Web Admin and allows the modification of the automatic configuration defined via this menu. See Chapter 9 : Configuring the DHCP server integrated MiVoice 5000 systems : for more information on how to manually configure the DHCP server.**

```
 *-------------------------------------------------*
| SUBNET MASK :                                     |
| BEGIN RANGE :                                     |
| END RANGE :                                       |
| GATEWAY :                                         |
| VLAN POSTE:                                       |
| VLAN PC :                                         |
*-------------------------------------------------*
Please_enter_valid_IP_BEGINRANGE
```

- Enter successively the configuration parameters of the integrated DHCP server, using the **Enter** key to change line.

```
*-------------------------------------------------------------------
----------*
| SUBNET MASK :       255.255.255.0                                 |
| BEGIN RANGE :       20.1.1.100                                    |
| END RANGE :         20.1.1.199                                    |
| GATEWAY :           20.1.1.254                                    |
| VLAN POSTE :                                                      |
| VLAN PC :                                                         |
*-------------------------------------------------------------------*
Do you confirm (Y/N) (Press enter to reconfigure) ? y
```

- Press "Y" to confirm the input.

Answer "**Y**" to the question:

```
Warning
Applying changes implies a iPBX restart
Do you want to apply your change Y(es) / N(o)/ R(econfigure)?
```

The procedure for configuring the system via **STANDARD RECONFIGURE** is completed and the system restarts.

### 6.10.8 RESTARTING MIVOICE 5000 SERVER

After the system is restarted, the automatic configuration phase last about 5 minutes.

During this period, the following main actions are taken:

- The DHCP server integrated to manage MiVoice 5300 IP Phone and Mitel 6000 SIP Phone (as well as i7xx) is automatically configured.
- The new network parameters of the integrated FTP server are taken into account in the integrated TMA, and the integrated FTP server accounts used by MiVoice 5300 IP Phone and Mitel 6000 SIP Phone automatically configured (see Chapters 6.5.2.4 and 6.5.2.5 ).
- The production software release of the integrated TMA is automatically configured with the software releases of Mitel 6000 SIP Phones and MiVoice 5300 IP Phones, contained in MiVoice 5000 R6.2.
- The global data configuration file used to deploy Mitel 6000 SIP Phones is updated with the information entered previously using **STANDARD RECONFIGURE.**
- Some automatic actions are automatically started by the integrated TMA to update the software releases and global data configuration file of MiVoice 5300 IP Phone and Mitel 6000 SIP Phone (respectively files localdb.config.ftp and aastra.cfg).

**Note : In factory presetting, the global data configuration file used to deploy Mitel 6000 SIP Phones is automatically updated with the country-location and operation information.**

**Note : The software releases of the Mitel 6000 SIP Phones and MiVoice 5300 IP Phones contained in MiVoice 5000 R6.2 are moved to the work directory of the integrated TMA (as of R5.4 SP1, some symbolic links are available in the directory deployment_67xxi: these symbolic links point to the TMA work directory or are stored in the software release of the production Mitel 6000 SIP Phone. There is no change for the global deployment configuration file aastra.cfg which remains physically present in this location).**

Automatic terminal configuration is enabled by default, as well as automatic update of the numbering plan and Mitel 6000 SIP Phone system keys, management of programmable keys, languages and pictures of Mitel 6000 SIP Phones (Menu Telephony service > Subscribers > Terminals and Applications > 6xxxi parameters).

The checks to be made before deploying MiVoice 5300 IP Phones and Mitel 6000 SIP Phones are indicated in the following sections.

To access the configuration menus of the integrated TMA, click the **Terminal service** menu from Web Admin.

### 6.10.9 CHECKING THE CONFIGURATION OF THE INTEGRATED DHCP SERVER ON MIVOICE 5000 SERVER

The **network** dedicated to MiVoice 5300 IP Phones, Mitel 6000 SIP Phones and i7xx is automatically configured using **STANDARD RECONFIGURE**.

All models of the terminals associated with these three terminal ranges can be configured for the **network.** The **network** is also automatically configured with the information entered during **STANDARD RECONFIGURE**.

- Subnet name
- Sub-network address
- Subnet mask
- IP address range
- Lease duration
- Router IP address.

For each terminal range concerned, the DHCP options are equally configured automatically using the information entered during **STANDARD RECONFIGURE**:

- Integrated FTP server IP address
- Main PBX IP address...

### 6.10.10 CHECKING THE CONFIGURATION OF THE INTEGRATED FTP SERVER ON MIVOICE 5000 SERVER

The storage directories used for daily management and deployment of MiVoice 5300 IP phones, Mitel 6000 SIP phones and MiVoice 5300 Digital phones are automatically created in the MiVoice 5000 Server. The main directory under which these directories are located is called **opt/a5000/infra/sip_sets**.

Each storage directory is accessible via an account (login/password) which defines the possible actions according to user type and terminal type.

The configuration of the integrated FTP server used by the integrated TMA is automatically defined and can be viewed in the **Servers configuration** menu (Action: **Modify**).



**Note : The fields Login/Write password and Login/Test Write password are not filled in because the integrated TMA uses some symbolic links to provide, in the right storage folders, the configuration software and files used by MiVoice 5300 IP Phone, Mitel 6000 SIP Phone and MiVoice 5300 Digital Phone.**

See Chapters 6.5.2.4 and 6.5.2.5 for the definition of the accounts used by MiVoice 5300 IP Phone and Mitel 6000 SIP Phone.

**For MiVoice 5300 Digital Phones**

The created directory is empty; it will be loaded later when these terminals are updated.

## 6.11 DEPLOYING MITEL 6000 SIP PHONES ON A NEW MIVOICE 5000 SERVER INSTALLATION

**Note : As from release R5.1C, Mitel 6000 SIP Phones can be managed from the integrated TMA.**

As of R6.2, it is possible to log on Mitel 6000 SIP Phone via the MiVoice 5000 User Portal application. A new global 6xxxi parameter is used to open this feature. The user selects a terminal on which to log on via the MiVoice 5000 User Portal application from its system label. For each terminal, this label is unique and automatically generated by the Mitel 5000 Gateways system. This label can be modified individually or massively.

As of R6.2, a global parameter can be configured to disable the free seating function. In this case (parameter unticked, the impact is as follows:

- On Mitel 6000 SIP Phones, the Ident key is no longer displayed, and manual login from the terminals is rejected for all the Mitel 6000 SIP Phones on the installation.

This parameter is accessible via Menu **Telephony service** > **Subscribers** > **Terminals and Applications** > **6xxxi parameters**, and is called **Manual login authorisation on any terminal type**. By default, this parameter is enabled (ticked). This parameter is accessible if login via MiVoice 5000 User Portal is open.

As of R6.2, a new tool for deploying Mitel 6000 SIP Phones through automatic login is configurable by automatically assigning a directory number to each terminal identified by its unique label. Automatic login is carried out next time the terminal is registered. This tool concerns all the (secure and unsecured) subscriptions.

As of R6.2, it is possible to secure or not the login tool during the Mitel 6000 SIP Phone deployment phase. A new subscription parameter is used to carry out this configuration:

- In non-secure mode, the parameter **Login via PC only** is not ticked (default value): the user can log on manually via the Ident key or via the corresponding feature code (*44 by default).
- In secure mode, the parameter **Login via PC only** is ticked: the user cannot log on manually via the Ident key or via the corresponding feature code (*44 by default).

As of R6.2, it is possible to reinforce the security of the MiVoice 5000 User Portal access by configuring and using Single Sign-on (SSO) mode (see document AMT/PTD/PBX/0080* for how to configure SSO mode).

After the pre-configuration made in Chapter 6.6, Mitel 6000 SIP Phones can be deployed using the following methods:

- Deployment through manual login on the terminal (**as of R5.2 only)**
- Deployment via MiVoice 5000 User Portal from a unique label identifying the terminal (**as of R6.2 only)**
- Automatic deployment by assigning a subscription number to the terminal (**as of R6.2 only)**
- Deployment from a dedicated Excel file

## 6.12 INVENTORY OF MITEL 6000 SIP PHONES

See Chapter 6.8.6 for the inventory of Mitel 6000 SIP Phones.

## 6.13 DEPLOYING MIVOICE 5300 IP PHONES ON A NEW MIVOICE 5000 SERVER INSTALLATION

**Note : As from release R5.1C, MiVoice 5300 IP Phones can be managed from the integrated TMA.**

As of R6.2, a global parameter can be configured to disable the free seating function. In this case (parameter unticked, the impact is as follows:

- On Mitel 5300 SIP Phones, the Ident key remains displayed, but manual login from the terminals is rejected for all the Mitel 5300 SIP Phones on the installation.

This parameter is accessible via Menu **Telephony service** > **Subscribers** > **Terminals and Applications** > **6xxxi parameters**, and is called **Manual login authorisation on any terminal type**. By default, this parameter is enabled (ticked). This parameter is accessible if login via MiVoice 5000 User Portal is open.

After the pre-configuration made in Chapter 6.10 , MiVoice 5300 IP Phones can be deployed using the following three methods:

- Automatic deployment through manual login on the terminal
- Deployment from a dedicated Excel file

See Chapter 6.9 for the deployment of MiVoice 5300 IP Phones.

## 6.14 INVENTORY OF MIVOICE 5300 IP PHONES

See Chapter 6.9.3 for the inventory of MiVoice 5300 IP Phones.

# 6.15 UPDATING MITEL 6000 SIP PHONES MANUALLY

## 6.15.1 PRINCIPLE

This chapter describes how to manually update Mitel 6000 SIP Phones.

Once a Mitel 6000 SIP Phone is known in the TMA inventory, this terminal is managed by TMA, and it can be updated on a daily basis.

**Note : Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.**

**Note : Mitel 6000 SIP Phone software and global data can be updated without any Mitel 6000 SIP Phone being physically connected to the network.**

The terminal may also be updated **automatically** while updating the iPBX (see Section 6.25).

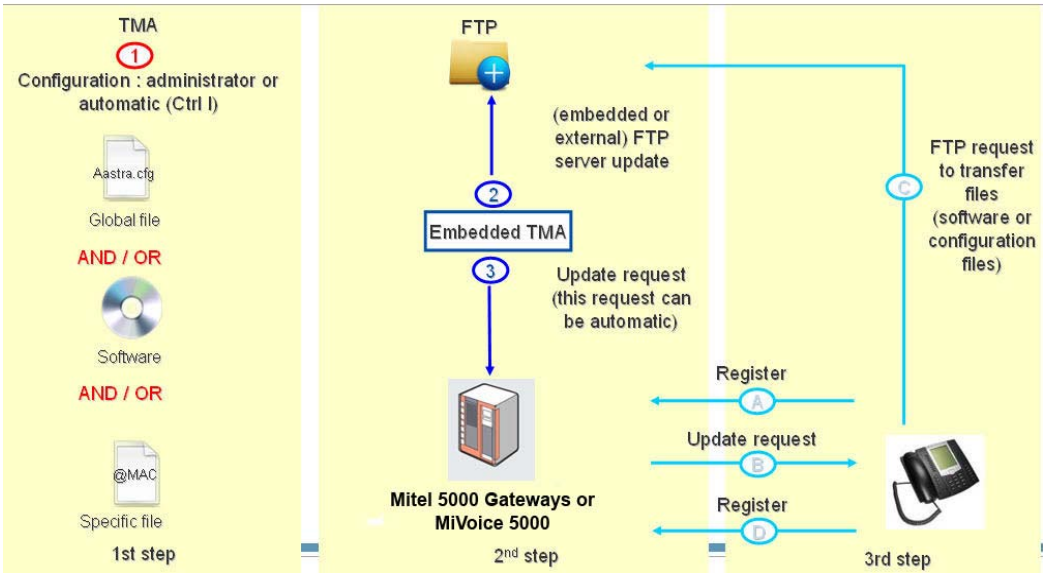
The update may concern:

- **Mitel 6000 SIP Phone software update**
  - Mitel 6000 SIP Phone software update concerns all Mitel 6000 SIP Phones, regardless of the their model and corresponds to updating the software.
- **Mitel 6000 SIP Phone global data update**
  - Mitel 6000 SIP Phone global data update concerns all Mitel 6000 SIP Phones, regardless of the their model.
- **Mitel 6000 SIP Phone specific data update**
  - Mitel 6000 SIP Phone specific data update concerns all Mitel 6000 SIP Phones, regardless of the their model. This update applies to a list of terminals which may contain one, several terminals or all the terminals of a site.

**Note : Updating the terminal data requires distributing the parameters first (refer to Section 6.15.5).**

**Note : See Section 6.15.6 for terminal list management.**

The diagram below illustrates the general principle of Mitel 6000 SIP Phone update.




- **The first step** consists in:
  - Installing a new terminal software release in TMA
  - Updating the terminals' global data in TMA
  - Updating the terminals' specific data in TMA
- **The second step** consists in starting the following operations from TMA:
  - Terminal software release update
  - Terminal global data update
  - Specific data update for terminals on a list

**Note : All or part of these three actions may be started consecutively.**

This update operation makes it possible to place the following data in the storage directory of the FTP server concerned:

- The new terminal software release
- The new terminal global data file
- The new terminal specific data files on a list.

For each set of data managed, an indicator (version or index) is used to identify the transmitted file without ambiguity.

**Note : All or part of this data may be available in the storage directory, depending on the actions started previously.**

This update operation also updates in the PBX:

- Information about the new terminal release to update
- The new values of the global and specific data index.

- **The third step** will enable the terminal to be updated automatically:
  - Next time the REGISTER is transmitted by the terminal, the data contained in the REGISTER is returned to the PBX. This data contains, among others, the current version of the terminal and the current values of the terminal's global and specific data index.
  - The PBX compares this terminal data with the data stored and saved previously in the PBX in step 2.
  - If at least any set of this data is different, the PBX transmits to the terminal an update order containing the IP address of the FTP server to which to connect, the account to use and the type of update to make.
  - This update order is followed by a terminal restart order. The terminal will then connect to the right FTP server and transfer the files concerned by the type of ordered update to the terminal.



**ATTENTION : The processing method used by TMA is asynchronous. The terminal update order also depends on REGISTER reception, the default rate of which is 1 hour.**

### 6.15.2 GLOBAL DATA UPDATE

This procedure applies once a terminal appears in the TMA application inventory. This procedure updates the global data of all the Mitel 6000 SIP Phones.



**Note : In R5.3 and later, logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.**

- Click the **Terminal configuration** menu.
- Select the **6xxxi** range.
- In the field **Version to configure**, select the version concerned by the global data update.
- Click the link **Modify global parameters**:
- A new window opens.

  This enables you to check which criteria are concerned by global data update:
  - The **terminal range**: **6xxxi**
  - The **Telephone set model** concerned: **all models**
  - The terminal **software** concerned
  - The **list** of terminals concerned: **fichier_global** (this information indicates that the global data update concerns all Mitel 6000 SIP Phones known in the TMA inventory for this multi-site configuration).

  As of R6.1 SP1, a distribution of the parameters in form of tabs is only displayed for Mitel 6000 SIP Phones: :
  - **Encryption**: encryption parameters for Mitel 6000 SIP Phones
  - **Config**: the usual configuration parameters
  - **TimeZone**: date and time, NTP server, time zone configuration parameters
  - **Network**: network parameters (DHCP, VLAN, LLDP,..)
  - **RFC2833**: RFC2833 / SIP INFO configuration parameters
  - **802.1X**: 802.1X configuration parameters

- **RTCP**: RTCP configuration parameters
- **Directory**: configuration parameters used to access the LDAP directory and Exchange contacts (function available as of R6.2)
- **Expert**: all the other parameters not available in the previous tabs.

This window also presents a table containing four columns:

- The **Parameters** column lists the parameters contained in the global data configuration file available in TMA. This list is from the distribution made previously.
- The **Default values** column displays the default values of the parameters contained in the factory description file available in TMA.
- The **Current values** column displays the current values of the parameters contained in the global data configuration file available in TMA.



**Note : Pop-ups give information on how to enter the value of each of the parameters. These latter appear when the cursor is placed over the current value of the parameter.**



**ATTENTION : After manual deployment via TMA, these values will be those imported via the global .csv file. For a deployment through manual login, these values will be the ones contained by default in the factory description.**

- The **Values to transfer** column displays the values to update in the global data configuration file available in TMA.

- Update the value of the parameter concerned in the **Values to transfer** column then click **Next**.



**Note : The Default values button is used to initialise the values to transfer with the default values for the tab in question.**



**Note : The modified parameters appear on a yellow background. A consistency check is made when the value of a parameter is entered. Incorrect parameters appear on a red background (value outside limit, for example).**

- A new window opens.

  This indicates the criteria concerned by global data update:

  - The **Multisite** concerned
  - The **terminal range**: **6xxxi**
  - The **Telephone set model** concerned: **all models**
  - The terminal **software** concerned
  - The **list** of terminals concerned: **fichier_global** (this information indicates that the global data update concerns all Mitel 6000 SIP Phones known in the TMA inventory).

The **Number of global data files to transfer** is also indicated.

- Enter the **Action name**.
- Select the **Type of update**:
  - Immediate
  - Deferred: specify the date in DD/MM/YYYY format and time in HHMM format.

**Note : Clicking the icon opens the calendar so the date can be selected directly.**

- Click **Confirm** to start global data update.

**ATTENTION : Any action started in deferred mode defers the transfer of data to the FTP server and the iPBX data update order.**

#### *6.15.2.1 Checking that the global data update process is working correctly*

This operation is used to ensure that the global data update operation has been performed correctly.

- Click the **Action monitoring** menu.
- Check in **Action monitoring,** the status of the global data update operation:
  - If the operation was successful, the status indicates: **Success**
- Click the icon to view the progress of the on-going global data update operation.
  - A colour code is used to check whether the terminal's global data is actually in the expected index (green colour) or not (red colour). This colour code is only significant for the last action of this type. The information displayed may or may not be filtered with this criterion.
- Check in the **Event log,** the status of the global data update operation.
  - If the operation was successful, the status indicates: **Action successful. Action on MiVoice 5000 PBX taken into account.**
  - The number of transferred files is used to check that the global file is actually placed in the storage directory of the FTP server used for day-to-day terminal management.
  - The report also indicates the system concerned by the action.

## 6.15.3 SPECIFIC DATA UPDATE

### *6.15.3.1 Updating common specific data*

This procedure applies once a terminal is registered on its reference site via any of the deployment methods described in the previous sections and when it appears in the TMA inventory. This procedure updates the common specific data of a list of Mitel 6000 SIP Phones. For example, if you wish to configure encryption for all the terminals on a list.

**Note : Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.**

**Note : See Section 6.15.6 for terminal list management.**

This procedure updates the specific data for a list of terminals.

Click the **Terminal configuration** menu.

- Select the **6xxxi** range.
- In the field **Version to configure**, select the version concerned by the specific data update.
- Click the link **Modify specific parameters**.
- A new window opens.

  This indicates the criteria concerned by specific data update:
  - The **terminal range**: **6xxxi**
  - The **Telephone set model** concerned: **all models**
  - The terminal **software** concerned
- Select the list of terminals concerned by the specific data update.

**Note : The "All" list is defined by default and contains all the terminals known to the inventory for the terminal range, the terminal model and multisite concerned. See Section 6.15.6 for list management.**

**Note : The greyed out values represent the canonical values of each parameter.**

As of R6.1 SP1, a distribution of the parameters in form of tabs is only displayed for Mitel 6000 SIP Phones:

- **Encryption**: encryption parameters for Mitel 6000 SIP Phones
- **Config**: the usual configuration parameters
- **TimeZone**: date and time, NTP server, time zone configuration parameters
- **Network**: network parameters (DHCP, VLAN, LLDP,..)
- **RFC2833**: RFC2833 / SIP INFO configuration parameters
- **802.1X**: 802.1X configuration parameters
- **RTCP**: RTCP configuration parameters
- **Directory**: configuration parameters used to access the LDAP directory and Exchange contacts (function available as of R6.2)
- **Expert**: all the other parameters not available in the previous tabs.

This window also presents a table containing three columns:

- When ticked, the **C** column is used to select a specific parameter for which the new value entered will be the same for all the terminals on the previously selected list.
- The **Parameters** column lists the parameters contained in the specific data configuration file available in TMA. This list is from the distribution made previously.
- The **Common values** column is used to enter the new value of a specific parameter selected via the **C** column.

**Note : Pop-ups give information on how to enter the value of each of the parameters. These latter appear when the cursor is placed over the current common value of the parameter.**

- Select one or more parameters then enter the new value for this parameter/these parameters.

**Note : A consistency check is made while validating the modifications. Incorrect parameters appear with a message specifying the expected format (values outside the limit, for instance).**

- Click **Save**. If no parameter is incorrect, a new window opens.

  This indicates the criteria concerned by specific data update:

  - The **terminal range**: **6xxxi**
  - The **Telephone set model** concerned: **all models**
  - The terminal **software** concerned
  - The **list** of terminals concerned

  This window also presents a table containing five columns:

  - When ticked, the **C** column is used to select one or more terminals for which some specific data will be entered if necessary based on terminals (see next chapter for implementation).
  - The other columns display the subscription **Number**, **Software release**, **IP address** and **MAC address** of each terminal on the previously selected list.
- Do not tick any terminal in the **C** column then click **Confirm**.
- A new window opens.

  This indicates the criteria concerned by specific data update:

  - The **terminal range**: **6xxxi**
  - The **Telephone set model** concerned: **all models**
  - The terminal **software** concerned
  - The **list** of terminals concerned.

The **Number of specific data files to transfer** is also indicated.

- Enter the **Action name**.
- Select the **Type of update**:
  - Immediate
  - Deferred: specify the date in DD/MM/YYYY format and time in HHMM format.

**Note : Clicking the icon opens the calendar so the date can be selected directly.**

- Click **Confirm** to start specific data update for a list of terminals.

**ATTENTION : Any action started in deferred mode defers the transfer of data to the FTP server and the iPBX data update order.**

### 6.15.3.2 *Specific data update*

This procedure updates the particular specific data of one or more terminals on a list of terminals. For example, if you wish to update the VLAN_ID of a list of terminals.

- Click the **Terminal configuration** menu.
- Select the **6xxxi** range.
- In the field **Version to configure**, select the version concerned by the specific data update.
- Click the link **Modify specific parameters**.
- A new window opens.

  This indicates the criteria concerned by specific data update:

  - The **terminal range**: **6xxxi**
  - The **Telephone set model** concerned: **all models**
  - The terminal **software** concerned
- Select the list of terminals concerned by the individual specific data update.

**Note : The "All" list is defined by default and contains all the terminals known to the inventory for the terminal range, the terminal model and multisite concerned. See Chapter 6.15.6 for list management.**

**Note : The greyed out values represent the canonical values of each parameter.**

As of R6.1 SP1, a distribution of the parameters in form of tabs is only displayed for Mitel 6000 SIP Phones:

- **Encryption**: encryption parameters for Mitel 6000 SIP Phones
- **Config**: the usual configuration parameters
- **TimeZone**: date and time, NTP server, time zone configuration parameters
- **Network**: network parameters (DHCP, VLAN, LLDP,..)
- **RFC2833**: RFC2833 / SIP INFO configuration parameters
- **802.1X**: 802.1X configuration parameters
- **RTCP**: RTCP configuration parameters
- **Directory**: configuration parameters used to access the LDAP directory and Exchange contacts (function available as of R6.2)
- **Expert**: all the other parameters not available in the previous tabs.

This window also presents a table containing four columns. Their meaning is described in the previous chapter.

- If possible, select one or more parameters then enter the new value for this parameter/these parameters.
- Click **Save**: a new window opens.

  This indicates the criteria concerned by specific data update:

  - The **terminal range**: **6xxxi**
  - The **Telephone set model** concerned: **all models**
  - The terminal **software** concerned
  - The **list** of terminals concerned

  This window also presents a table containing five columns:

  - when ticked, the **C** column is used to select one or more terminals for which some particular specific data will be entered based on terminals.
  - The other columns display the subscription **Number**, **Software release**, **IP address** and **MAC address** of each terminal on the previously selected list.
- Select one, more or all the terminals by ticking them in the **C** column.
- Click **Validate**.
- A new window opens.

  This indicates the criteria concerned by specific data update:

  - The **terminal range**: **6xxxi**
  - The **Telephone set model** concerned: **all models**
  - The terminal **software** concerned
  - The **list** of terminals concerned.
  - The subscription **number** concerned
  - The **MAC address** of the subscription concerned.

  This window also presents a table containing four columns, based on tabs.

  - The **Parameters** column lists the parameters contained in the specific data configuration file available in TMA. This list is from the distribution made previously.
  - The **Default values** column displays the default values of the parameters contained in the factory description file available in TMA.
  - The **Current values** column displays the current values of the parameters contained in the specific data configuration file of the terminal concerned, available in TMA.



**ATTENTION : After manual deployment via TMA, these values will be those imported via the specific .csv file. For a deployment through manual login, these values will be the ones contained by default in the factory description.**

  - The **Values to transfer** column displays the values to update in the specific data configuration file of the terminal concerned in TMA.



**Note : Pop-ups give information on how to enter the value of each of the parameters. These latter appear when the cursor is placed over the current specific value of the parameter.**



**Note : The Default values button is used to initialise the values to transfer with the default values for the tab in question.**

- Update the value of the parameter(s) concerned in the **Values to transfer** column then click **Next** to go to the next terminal.

**Note : The Initialise button resets all the terminal parameters to their current value.**

**Note : The modified parameters appear on a yellow background. A consistency check is made when the value of a parameter is entered. Incorrect parameters appear on a red background (value outside limit, for example).**

- After modifying the last terminal selected, click **Create action**.
- A new window opens.

  This indicates the criteria concerned by specific data update:

  - The **terminal range**: **6xxxi**
  - The **Telephone set model** concerned: **all models**
  - The terminal **software** concerned
  - The **list** of terminals concerned.

  The **Number of specific data files to transfer** is also indicated.
- Enter the **Action name**.
- Select the **Type of update**:
  - Immediate
  - Deferred: specifies the date in DD/MM/YYYY format and time in HHMM format.

**Note : Clicking the icon opens the calendar so the date can be selected directly.**

- Click **Confirm** to start specific data update for a list of terminals.

**ATTENTION : Any action started in deferred mode defers the transfer of data to the FTP server and the PBX data update order.**

### *6.15.3.3 Checking that the specific data update process is working correctly*

This operation is used to ensure that the specific data update operation has been performed correctly.

- Click the **Action monitoring** menu.
- Check in **Action monitoring,** the status of the specific data update operation:
  - If the operation was successful, the status indicates: **Success**
- Click the icon to view the progress of the on-going specific data update operation.
  - A colour code is used to check whether the terminal's specific data is actually in the expected index (green colour) or not (red colour). This colour code is only significant for the last action of this type. The information displayed may or may not be filtered with this criterion.
- Check in the **Event log** the status of the specific data update operation.
  - If the operation was successful, the status indicates: **Action successful. Action on MiVoice 5000 PBX taken into account.**
  - The number of transferred files is used to check that all the specific files are actually placed in the storage directory of the FTP server used for day-to-day terminal management. The report also indicates the system concerned by the action.

## 6.15.4 UPDATING MITEL 6000 SIP PHONE SOFTWARE RELEASE

This procedure allows the software release of all Mitel 6000 SIP Phones to be updated..

**Note : Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.**

### *6.15.4.1 Installing the new software release to be deployed*

New packages must have been uploaded to the Repository server.

As of R6.5, only the Repository Update method allows the software update of the stations.

Refer to the document Updating by -Repository AMT / PTD / PBX / 0155/2 (Minimum Edition 2 for R6.5).

The embedded TMA application then connects directly to the repository server to list available "terminal" packages

- Click the **Software management** menu.
- Select the **6xxxi** range.
- Click **Change**.
- Click the **Add versions** link:

This action polls the repository server.

After selection of the range, a list selection shows the available packages on the server.

A new window opens showing the list of available Software Versions.

- Select the version considered,

Once the version is selected, the list of components present in this package is presented.

The components corresponding to the managed models are preselected.

- Tick or untick if necessary the models of terminals to update.
- Click on **Download**.

Downloading software updates is then launched to the iPBX for managed models.

Once the download is successful, close the window;

The new versions are available to be configured, either in production version or in test version on the positions considered. Refer to the following paragraphs.

### 6.15.4.2 *Defining the new production release*

This procedure is used to define the new production software release.

- Click the **Software management** menu.
- Select the **6xxxi** range.
- Click **Change**.
- Click the link **Configure production software release**:
  - Select the new version and click **Validate**.

**Note : The new software release is now the production release and all the terminals appear in red in the inventory (terminals seen in another software release).**

### 6.15.4.3 *Starting the update of the new production release*

- Click **Return**.
- A new window opens.

  This indicates the criteria concerned by the update of the new software release:
  - The **terminal range**: **6xxxi**
  - The **Production software release**concerned
- Enter the **Action name**.
- Select the **Software release** concerned.
- Select the **Type of update**:
  - Immediate
  - Deferred: specify the date in DD/MM/YYYY format and time in HHMM format.

**Note : Clicking the icon opens the calendar so the date can be selected directly.**

- Click **Validate** to start updating the software release of all Mitel 6000 SIP Phones.

#### 6.15.4.4 *Checking that the production software release update is working correctly*

This operation is used to ensure that the new software release has been correctly updated.

- Click the **Action monitoring** menu.
- Check in **Action monitoring,** the status of the production release update operation:
  - If the operation was successful, the status indicates: **Success**
- Click the icon to view the progress of the on-going production release update operation.
  - A colour code is used to check whether the terminals have the expected software release (green colour) or not (red colour). This colour code is only significant for the last action of this type. The information displayed may or may not be filtered with this criterion.
- Check in the **Event log** the status of the terminal software release update operation.
  - If the operation was successful, the status indicates: **Action successful. Action on MiVoice 5000 PBX taken into account.**
  - The number of transferred files is used to check that all new software release files have actually been placed in the storage directory of the FTP server used for day-to-day terminal management. The system concerned by the action is also indicated.

### 6.15.5 DISTRIBUTING THE NEW PRODUCTION RELEASE PARAMETERS

This procedure is used to distribute the parameters associated with a new software release installed in TMA. The range of each parameter is given.

A parameter is defined either:

- In the Mitel 6000 SIP Phone global data configuration file
- In the Mitel 6000 SIP Phone specific data configuration file
- In the DHCP server
- Or in none of the previous ranges, so this parameter is not managed.

This distribution must be made for each software release installed and configured in TMA as production release or test release.

- Click the **Terminal configuration** menu.
- Select the **6xxxi** range.
- In the field **Version to configure**, select the version concerned by the distribution.

  As of R6.1 SP1, a distribution of the parameters in form of tabs is only displayed for Mitel 6000 SIP Phones:
  - **Encryption**: encryption parameters for Mitel 6000 SIP Phones
  - **Config**: the usual configuration parameters
  - **TimeZone**: date and time, NTP server, time zone configuration parameters
  - **Network**: network parameters (DHCP, VLAN, LLDP,..)
  - **RFC2833**: RFC2833 / SIP INFO configuration parameters
  - **802.1X**: 802.1X configuration parameters
  - **RTCP**: RTCP configuration parameters
  - **Directory**: configuration parameters used to access the LDAP directory and Exchange contacts (function available as of R6.2)

- **Expert**: all the other parameters not available in the previous tabs.

**Note : To facilitate the introduction of certain features (encryption, etc.), some parameters are available twice in the tab:**
**- in the upper part, the parameters have a range and some fixed values.**
**- in the lower part, the same parameters have a default value which may differ and a range set to ignored.**

- Select a tab then define its range for each parameter available in this tab.

**Note : After the iPBX is upgraded, the range defined in software release n-1 is kept in terminal software release n. The range of the new parameters introduced in the new terminal software release must be defined.**

- Click **Save**:
  - Clicking **Distribute** displays a confirmation message before the distribution of parameters is locked for this software release.
  - The **Initialise** button restores the factory distribution of the parameters associated with this software release.

**Note : The parameters managed by DHCP, or ignored, are displayed for information purposes only.**

**Note : In release R5.3 and later, it is possible to unlock the distribution of parameters and make a new distribution. In this case, the global and specific data must be updated in order to update the values of the parameters whose assignment has been changed.**

### 6.15.6 MANAGING THE LIST OF TERMINALS FOR MITEL 6000 SIP PHONES

This procedure is used to define a list of terminals for all models of Mitel 6000 SIP Phones.

This list is used either:

- In nominal mode, to update some specific data on a global or restricted range, or
- In test mode, to update the terminals' software release, global data and specific data on a limited range.

**ATTENTION : In test mode, the list contains a maximum of 10 terminals.**

**ATTENTION : A terminal may be assigned only to one list at a time.**

The list used in test mode to update the terminal software release must be the same as the one used to update the global data and specific data.

### 6.15.6.1 *Defining a new list by entering the terminals one by one*

- Click the **Inventory** menu.
- Select the **67xxi range** and possibly the **model**.
- Click **List management:**

  A new window opens. This window gives the criteria concerned by the list creation:

  - The **terminal range**: **6xxxi**
  - The Telephone set **model** concerned
- Click **Add new list**.

A new window opens. This window allows you to enter one by one the terminals contained on the list.

- In the right input area, for each terminal to be added to the list, enter the directory number of the terminal then click **Add set**.

**Note : To delete a terminal from the currently edited list, select the terminal then click Delete.**

- In the right area, enter the **List name** then click **Confirm**.
  - The message has been successfully saved.
- Close the window either by clicking the **Close window** link, or by clicking on the top right side of the window.
- The list management window is refreshed and then displays:
  - The list name
  - The number of terminals contained on the list
  - The **Action** field used to delete or modify the displayed list.
- Click **Return** to return to the **Inventory** window.

### 6.15.6.2 *Modifying a list*

- Click the **Inventory** menu.
- Select the **67xxi range** and possibly the **model**.
- Click **List management:**

  A new window opens. This window gives the criteria concerned by the list creation:

  - The **terminal range**: **6xxxi**
  - The Telephone set **model** concerned
- In the **Action** field, click the icon of the list to modify.
- Modify the list by adding or deleting a terminal.
- Click **Confirm**.
  - The message has been successfully saved.
- Close the window either by clicking the **Close window** link, or by clicking on the top right side of the window.
- The list management window is refreshed and then displays:
  - The list name
  - The new number of terminals contained on the list
- Click **Return** to return to the **Inventory** window.

#### 6.15.6.3 *Deleting a list*

- Click the **Inventory** menu.
- Select the **67xxi range** and possibly the **model**.
- Click **List management:**

  A new window opens. This window gives the criteria concerned by the list creation:

  - The **terminal range**: **6xxxi**
  - The Telephone set **model** concerned

- In the **Action** field, click the ✗ icon of the list to delete:
  - a confirmation message is displayed so you can confirm or cancel the list deletion.
- The list management window is refreshed and the deleted list no longer appears.
- Click **Return** to return to the **Inventory** window.

## 6.16 TEST MODE FOR MITEL 6000 SIP PHONES

The test mode is used to update the terminals' software release, global data and specific data on a range limited to 10 terminals maximum. This function is used to test a new terminal software application or new function/configuration on a small number of terminals before exposing it to all the terminals.

The list of terminals used in test mode to update the terminal software release must be the same as the one used to update the global data and specific data of the tested terminals.

The different files (terminal software, global or specific data) are stored in the **test directory** defined in the FTP server configuration.

### 6.16.1 UPDATING MITEL 6000 SIP PHONE SOFTWARE RELEASE IN TEST MODE

This procedure applies once a terminal is registered on its reference site via any of the deployment methods described in the previous chapters and when it appears in the TMA inventory. This procedure is used to update the software release of the Mitel 6000 SIP Phones known to the inventory and defined on a list containing at most 10 terminals.

In the example below:

- The production release = **R6.2_67xxi_A5_00**
- The test release = **R6.2_67xxi_A6_00**



**ATTENTION : In test mode, only one software release update operation can be performed at a time for a list of terminals.**

#### 6.16.1.1 *Defining a test list*

See Section 6.15.6 for how to define a list of terminals containing a maximum of 10 terminals.

This list, called **test** , will be used in the procedure described below.



**ATTENTION : A list used by an on-going test cannot be deleted or modified.**

#### 6.16.1.2 *Installing the new test software release*

To install the new software release to be updated, use the MiVoice 5000 R6.2 software CD-ROM containing the new software release then proceed as follows:

- Place the MiVoice 5000 R6.2 software DVD or CD-ROM in the drive of the PC accessing Web

Admin.

- Click the **Software management** menu.
- Select the **6xxxi** range.
- Click **Change**.
- Click the **Add versions** link:

  a new window opens, showing the list of installed software releases. By default, this list is empty.
- Click **Browse**.
  - Go to the **sip_sets_tma** directory of the MiVoice 5000 R6.2 software CD-ROM.
  - Select the corresponding tar.gz file for the software package to be installed. The file **R6.2_67xx-i_A6_00.tar.gz** corresponds, for instance, to the test terminal software package. Click **Open.**
  - Click Send: the terminal version is installed and then appears on the list of installed software releases. Close the window by clicking on the top right side of the window.

#### *6.16.1.3 Defining the new test release*

This procedure is used to define the new test software release.

- Click the **Software management** menu.
- Select the **6xxxi** range.
- Click **Change**.
- Click the link **Configure test software release**:
  - select the previously installed terminal software package **R6.2_67xxi_A6_00** then click **Validate**.

**Note : Terminal software package R6.2_67xxi_A6_00 is now the test terminal software package.**

#### *6.16.1.4 Starting the update of the new test version*

- Click **Return**.
- A new window opens.

  This indicates the criteria concerned by the update of the new software release:
  - The **terminal range**: **6xxxi**
  - The **Production software release**concerned: **R6.2_67xxi_A5_00**
  - The **Test software release**concerned: **R6.2_67xxi_A6_00**

**Note : The Details button is used to know the content of the terminal software package.**

- Enter the **Action name**.
- Select the test **Software release** concerned: **R6.2_67xxi_A6_00**

- Select the list to use in test mode: **test**
  - The **List details** link is used to display the terminals contained on the selected list.
- Select the **Type of update**:
  - Immediate
  - Deferred: specify the date in DD/MM/YYYY format and time in HHMM format.

**Note : Clicking the icon opens the calendar so the date can be selected directly.**

- Click **Validate** to start updating the software release of all Mitel 6000 SIP Phones.

#### 6.16.1.5 *Checking that the test software release update is working correctly*

This operation is used to ensure that the new test software release has been correctly updated.

- Click the **Action monitoring** menu.
- Check in **Action monitoring,** the status of the test version update operation: if the operation is successful, the status displays: **Success**
- Click the icon to view the progress of the on-going test software release update operation.
  - A colour code is used to check whether the terminals have the expected software release (green colour) or not (red colour). This colour code is only significant for the last action of this type. The information displayed may or may not be filtered with this criterion.
  - The **List** field displays the list used in test mode: **test**
  - The **Test** field is used to check whether or not the on-going operation is in test mode.
- Check in the **Event log** the status of the test software release update operation.
  - If the operation was successful, the status indicates: **Action successful. Action on MiVoice 5000 PBX taken into account.**
  - The number of transferred files is used to check that all new test software release files have actually been placed in the test storage directory of the FTP server used for day-to-day terminal management in test mode.

### 6.16.2 DISTRIBUTING THE NEW TEST SOFTWARE RELEASE PARAMETERS

See Chapter 6.15.5 for how to define the distribution of the new test software release parameters.

### 6.16.3 UPDATING THE GLOBAL DATA OF TERMINALS IN THE TEST SOFTWARE RELEASE

This procedure is used to update the global data of Mitel 6000 SIP Phone in the test software release.

- Click the **Terminal configuration** menu.
- Select the **6xxxi** range.
- In the field **Version to configure**, select the test version concerned by the global data update (**R6.2_67xxi_A6_00** in the example).
- Click the link **Modify global parameters**:
- A new window opens.

  This enables you to check which criteria are concerned by global data update on the test software release:
  - The **terminal range**: **6xxxi**
  - The **Telephone set model** concerned: **all models**

- The terminal **software** concerned: **R6.2_67xxi_A6_00**
- The **list** of terminals concerned: **test** (this information shows that the global data update applies to the **test** list, currently used in test mode). The **List details** link is used to display the terminals contained in the selected list.

- See Section Global data update for information on how to program the global data update in test mode, except that the list concerned by the action is not the global-file list but the list in test mode, called test in our example.

#### *6.16.3.1 Checking that the global data update process is working correctly in test mode*

This operation is used to ensure that the global data update in test mode has been performed correctly.

- Click the **Action monitoring** menu.
- Check in **Action monitoring,** the status of the global data update on the terminals in test mode: if the operation is successful, the status displays: **Success**
- Click the  icon to view the progress of the on-going global data update operation.
  - The **List** field displays the list used in test mode: **test**
  - The **Test** field is used to check whether or not the on-going operation is in test mode.
  - A colour code is used to check whether the terminal's global data is actually in the expected index (green colour) or not (red colour). This colour code is only significant for the last action of this type. The information displayed may or may not be filtered with this criterion.
- Check in the **Event log** the status of the global terminal data update in test mode.
  - If the operation was successful, the status indicates: **Action successful. Action on MiVoice 5000 PBX taken into account.**
  - The number of transferred files is used to check that the global file has actually been placed in the test storage directory of the FTP server used for terminal test mode.

## 6.16.4 UPDATING THE SPECIFIC DATA OF INDIVIDUAL TERMINALS USED WITH THE TEST SOFTWARE

This procedure is used to update the specific data of Mitel 6000 SIP Phone in the test software release.

### *6.16.4.1 Updating the specific data common to all terminals used with the test software*

This procedure is used to update the specific data of terminals in the test software release.

- Click the **Terminal configuration** menu.
- Then select the **6xxxi** range.
- In the field **Version to configure**, select the test version concerned by the specific data update. (**R6.2_67xxi_A6_00** in the example).
- Click the link **Modify specific parameters**.
- A new window opens.

  This indicates the criteria concerned by specific data update:

  - The **terminal range**: **6xxxi**
  - The **Telephone set model** concerned: **all models**
  - The terminal **software** concerned: **R6.2_67xxi_A6_00**
  - The **list** of terminals concerned: **test** (this information shows that the specific data update applies to the **test** list, currently used in test mode).



**Note : It is not possible in test mode to start a specific data update operation on the production release using the "All" list.**

See Section 6.15.3.1 for information on how to program the common specific data update in test mode, except that the list concerned by the action is the list in test mode, called test in our example.

### 6.16.4.2 *Updating the special specific data of terminals in the test software release*

This procedure is used to update the special specific data of terminals in the test software release.

- Click the **Terminal configuration** menu.
- Then select the **6xxxi** range.
- In the field **Version to configure**, select the test version concerned by the specific data update. (**R6.2_67xxi_A6_00** in the example).
- Click the link **Modify specific parameters**.
- A new window opens.

  This indicates the criteria concerned by specific data update:

  - The **terminal range**: **6xxxi**
  - The **Telephone set model** concerned: **all models**
  - The terminal **software** concerned: **R6.2_67xxi_A6_00**
  - The **list** of terminals concerned: **test** (this information shows that the specific data update applies to the **test** list, currently used in test mode).



**Note : It is not possible in test mode to start a specific data update operation on the production release using the "All" list.**



**Note : The greyed out values represent the canonical values of each parameter.**

See Section 6.15.3.2 for information on how to program the individual specific data update in test mode, except that the list concerned by the action is the list in test mode, called test in our example.

### 6.16.4.3 *Checking that the specific data update process is working correctly in test mode*

This operation is used to ensure that the specific data update in test mode has been performed correctly.

- Click the **Action monitoring** menu.
- Check in **Action monitoring,** the status of the specific data update in test mode: if the operation is successful, the status displays: **Success**
- Click the icon to view the progress of the on-going specific data update operation.
  - The **List** field displays the list used in test mode: **test**
  - The **Test** field is used to check whether or not the on-going operation is in test mode.
  - A colour code is used to check whether the terminal's specific data is actually in the expected index (green colour) or not (red colour). This colour code is only significant for the last action of this type. The information displayed may or may not be filtered with this criterion.
- Check in the **Event log** the status of the specific data update operation.
  - If the operation was successful, the status indicates: **Action successful. Action on MiVoice 5000 PBX taken into account.**
  - The number of transferred files is used to check that all the specific files have actually been placed in the test storage directory of the FTP server used for terminal test mode.

## 6.16.5 EXITING THE TEST MODE

This procedure is used to leave the test mode at the end of the test phase.

Two possibilities are available:

- The tested new software release is satisfactory: in this case, all the terminals on the installation must be updated with the new test software.
- The tested new software release is not satisfactory: in this case, only the tested terminals must be updated with the current production software.

### *6.16.5.1 Switching from test mode to production mode*

In this case, the test software release must be defined as the new production software release, and an update operation for this new production software release started on all the terminals.

In the example below the initial situation is as follows:

  - production release = **R6.2_67xxi_A5_00**
  - test release = **R6.2_67xxi_A6_00**
- Click the **Software management** menu.
- Select the **6xxxi** range.
- Click **Change**.
- Click the link **Configure production software release**:
  - Select the release **R6.2_67xxi_A6_00** and click **Validate**.

  the situation is now:
  - production release = **R6.2_67xxi_A6_00**
  - No test version defined.
- Click **Return**.
- A new window opens.

  This indicates the criteria concerned by the update of the new software release:
  - The **terminal range**: **6xxxi**
  - The **Production software release**concerned: **R6.2_67xxi_A6_00**
- Enter the **Action name**.
- Select the **Software release** concerned: **R6.2_67xxi_A6_00**
- Select the **Type of update**:
  - Immediate
  - Deferred: specifies the date in DD/MM/YYYY format and time in HHMM format.

**Note : Clicking the icon opens the calendar so the date can be selected directly.**

- Click **Validate** to start updating the production software release of all Mitel 6000 SIP Phones.

### 6.16.5.2 *Returning to the current version*

In this case, the test software release is not satisfactory. The terminals on the test list must be downgraded with the current production release. An update for this production software release must be started on all the terminals.

In the example below the initial situation is as follows:

- production release = **R6.2_67xxi_A5_00**
- test release = **R6.2_67xxi_A6_00**

- Click the **Software management** menu.
- Select the **6xxxi** range.
- Enter the **Action name**.
- Select the **Software release** concerned: **R6.2_67xxi_A5_00**
- Select the **Type of update**:
  - Immediate
  - Deferred: specifies the date in DD/MM/YYYY format and time in HHMM format.



**Note : Clicking the icon opens the calendar so the date can be selected directly.**

- Click **Validate** to start updating the current production software release of all Mitel 6000 SIP Phones.



**Note : Only the terminals with the test software release will be updated with the current production software release because all the other terminals are already in the right version.**

# 6.17 UPDATING MIVOICE 5300 IP PHONES MANUALLY

## 6.17.1 PRINCIPLE

This chapter describes how to manually update MiVoice 5300 IP Phones.

Once a MiVoice 5300 IP Phone is known in the TMA inventory, this terminal is managed by TMA, and it can be updated on a daily basis.

**Note : Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.**

**Note : MiVoice 5300 IP Phone software and global data can be updated without any MiVoice 5300 IP Phone being physically connected to the network.**

The terminal may also be updated **automatically** while updating the iPBX (see Section 6.25.1).

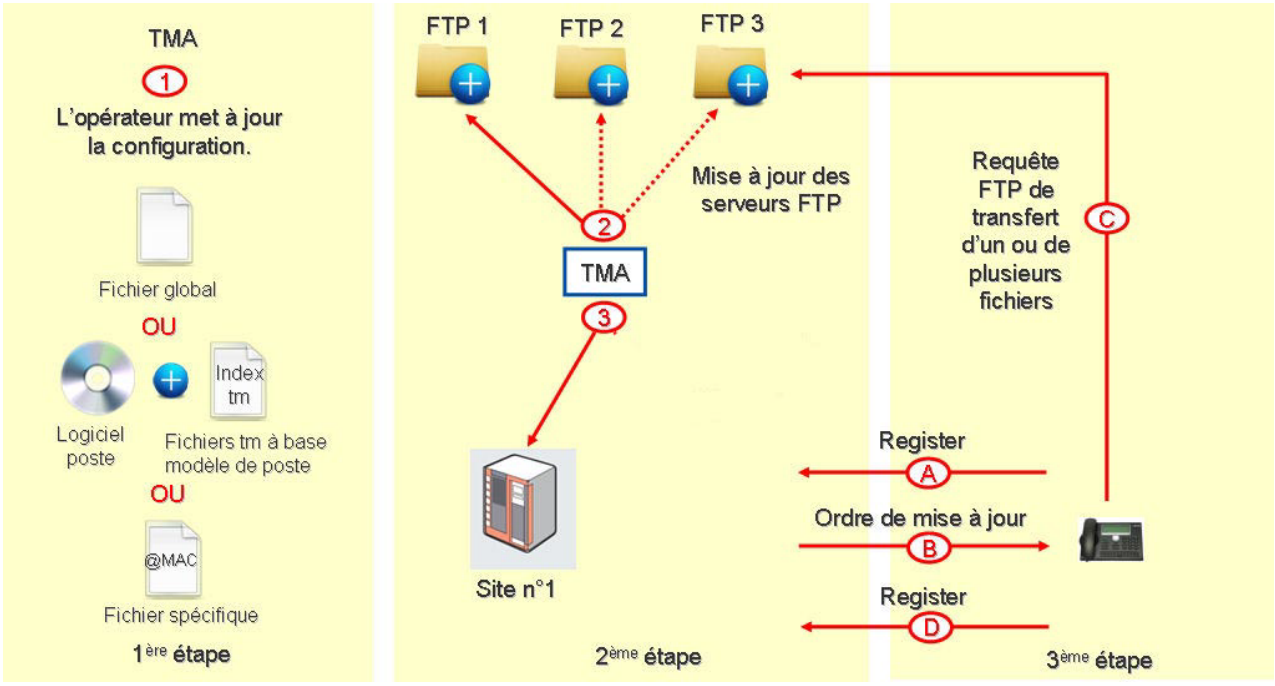
The update may concern:

- MiVoice 5300 IP Phone **software update**
  - MiVoice 5300 IP Phone software update concerns all MiVoice 5300 IP Phones, regardless of their model, and corresponds to software and TM (terminal model) data update.
- MiVoice 5300 IP Phone **global data update**
  - MiVoice 5300 IP Phone global data update concerns all MiVoice 5300 IP Phones, regardless of the their model.
- MiVoice 5300 IP Phone **specific data update**
  - MiVoice 5300 IP Phone specific data update concerns all MiVoice 5300 IP Phones, regardless of the their model. This update applies to a list of terminals which may contain one, several terminals or all the terminals of a site.

**Note : Updating the terminal data requires distributing the parameters first (refer to Section Distributing the new production release parameters page 153).**

**Note : See Section Managing the list of terminals for MiVoice 5300 IP Phones page 170 for terminal list management.**

The diagram below illustrates the general principle of MiVoice 5300 IP Phone update.




**ATTENTION : Delete from the FTP server the files indexed by their directory number if the FTP server is the same for daily deployment and management.**

- **The first step** consists in:
  - Installing a new terminal software release in TMA
  - Updating the terminals' global data in TMA
  - Updating the terminals' specific data in TMA
- **The second step** consists in starting the following operations from TMA:
  - Terminal software release update
  - Terminal global data update
  - Specific data update for terminals on a list

**Note : All or part of these three actions may be started consecutively.**

This update operation makes it possible to place the following data in the storage directory of the FTP server concerned:

- The new terminal software release
- The new terminal global data file
- The new terminal specific data files on a list.

For each set of data managed, an indicator (version or index) is used to identify the transmitted file without ambiguity.

**Note : All or part of this data may be available in the storage directory, depending on the actions started previously.**

This update operation also updates in the PBX:

- Information about the new terminal release to update
- The new values of the global and specific data index.

- **The third step** will enable the terminal to be updated automatically:
  - Next time the REGISTER is transmitted by the terminal, the data contained in the REGISTER is returned to the PBX. This data contains, among others, the current version of the terminal and the current values of the terminal's global and specific data index.
  - The PBX compares this terminal data with the data stored and saved previously in the PBX in step 2.
  - If at least any set of this data is different, the PBX transmits to the terminal an update order containing the IP address of the FTP server to which to connect, the account to use and the type of update to make.
  - This update order is followed by a terminal restart order. The terminal will then connect to the right FTP server and transfer the files concerned by the type of ordered update to the terminal.

**ATTENTION : The processing method used by TMA is asynchronous. The terminal update order also depends on REGISTER reception, the default rate of which is 1 hour.**

## 6.17.2 GLOBAL DATA UPDATE

This procedure applies once a terminal appears in the TMA application inventory. This procedure updates the global data of all the MiVoice 5300 IP Phones.

**Note : Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.**

See Chapter 6for details of the procedure, and use the following parameters:

- Select the **53xxip** range.

**Note : Tab-based parameter distribution is not available for MiVoice 5300 IP Phones.**

### *6.17.2.1 Checking that the global data update process is working correctly*

This operation is used to ensure that the global data update operation has been performed correctly.

See Chapter 6.15.2.1 for more details.

## 6.17.3 SPECIFIC DATA UPDATE

### *6.17.3.1 Updating common specific data*

This procedure applies once a terminal appears in the TMA application inventory. This procedure updates the common specific data of a list of MiVoice 5300 IP Phones.

**Note : Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.**

**Note : See Section 6.17.6 for terminal list management.**

See Chapter 6.15.3.1for details of the procedure, and use the following parameters:

- Select the **53xxip** range.

### *6.17.3.2 Updating individual specific data*

This procedure updates the particular specific data of one or more terminals on a list of terminals. For example, if you wish to update the VLAN_ID of a list of terminals as well as the VLAN_PRIO of a particular terminal on this same site.

See Chapter 6.15.3.2for details of the procedure, and use the following parameters:

- Select the **53xxip** range.

**Note : Tab-based parameter distribution is not available for MiVoice 5300 IP Phones.**

### *6.17.3.3 Checking that the specific data update process is working correctly*

This operation is used to ensure that the specific data update operation has been performed correctly.

See Chapter 6.15.3.3 for more details.

## 6.17.4 UPDATING MIVOICE 5300 IP PHONE SOFTWARE RELEASE

This procedure applies once a terminal appears in the TMA application inventory. This procedure is used to update the software release of all MiVoice 5300 IP Phones known to the inventory.

**Note : In R5.3 and later, logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.**

### *6.17.4.1 Installing the new software release to be deployed*

Refer to section 6.15.4.1

### *6.17.4.2 Defining the new production release*

This procedure is used to define the new production software release.

See Chapter 6.15.4.2 for details of the procedure, and use the following parameters:

- Select the **53xxip** range.

**Note : The new software release is now the production release and all the terminals appear in red in the inventory (terminals seen in another software release).**

### *6.17.4.3 Starting the update of the new production release*

See Chapter 6.15.4.3 for details of the procedure, and use the following parameters:

- Select the **53xxip** range.

### *6.17.4.4 Checking that the production software release update is working correctly*

This operation is used to ensure that the new software release has been correctly updated.

Refer to Chapter 6.15.4.4 for more information about the procedure.

### 6.17.5 DISTRIBUTING THE PARAMETERS OF THE NEW PRODUCTION RELEASE

This procedure is used to distribute the parameters associated with a new software release installed in TMA. The range of each parameter is given.

A parameter is defined either:

- In the MiVoice 5300 IP Phone global data configuration file
- In the MiVoice 5300 IP Phone specific data configuration file
- In the DHCP server
- Or in none of the previous ranges, so this parameter is not managed.

This distribution must be made for each software release installed and configured in TMA as production release or test release.

See Chapter 6.15.5 for details of the procedure, and use the following parameters:

- Select the **53xxip** range.

**Note : Tab-based parameter distribution is not available for the 53xxip range.**

**Note : The parameters managed by DHCP, or ignored, are displayed for information purposes only.**

## 6.17.6 MANAGING THE LIST OF TERMINALS FOR MIVOICE 5300 IP PHONES

This procedure is used to define a list of terminals for all models of MiVoice 5300 IP Phones.

This list is used either:

- In nominal mode, to update some specific data on a global or restricted range, or
- In test mode, to update the terminals' software release, global data and specific data on a limited range.



**ATTENTION : In test mode, the list contains a maximum of 10 terminals.**



**ATTENTION : A terminal may be assigned only to one list at a time.**

The list used in test mode to update the terminal software release must be the same as the one used to update the global data and specific data.

### *6.17.6.1 Defining a new list by entering the terminals one by one*

See Chapter 6.15.6.1 for details of the procedure, and use the following parameters:

- Select the **53xxip** range.

### *6.17.6.2 Modifying a list*

See Chapter 6.15.6.2 for details of the procedure, and use the following parameters:

- Select the **53xxip** range.

### *6.17.6.3 Deleting a list*

See Chapter 6.15.6.3 for details of the procedure, and use the following parameters:

- Select the **53xxip** range.

# 6.18 TEST MODE FOR MIVOICE 5300 IP PHONES

The test mode is used to update the terminals' software release, global data and specific data on a range limited to 10 terminals maximum. This function is used to test a new terminal software application or new function/configuration on a small number of terminals before exposing it to all the terminals.

The list of terminals used in test mode to update the terminal software release must be the same as the one used to update the global data and specific data of the tested terminals.

The different files (terminal software, global or specific data) are stored in the **test directory** defined in the FTP server configuration.

## 6.18.1 UPDATING MIVOICE 5300 IP PHONE SOFTWARE RELEASE IN TEST MODE

This procedure applies once a terminal is registered on its reference site following the deployment, and appears in the TMA application inventory. This procedure is used to update the software release of the MiVoice 5300 IP Phones known to the inventory and defined on a list containing at most 10 terminals.

In the example below:

- The production release = **R6.1_53xxip_E2_00**
- The test release = **R6.1_53xxip_E3_00.**

**ATTENTION : In test mode, only one software release update operation can be performed at a time for a list of terminals.**

### *6.18.1.1 Defining a test list*

See Section 6.11.8 - Managing MiVoice 5300 IP Phone lists - to define a list of terminals containing at most 10 terminals.

This list, called **test** , will be used in the procedure described below.

**ATTENTION : A list used by an on-going test cannot be deleted or modified.**

### *6.18.1.2 Installing the new test software release*

Refer to section 6.15.4.1

#### 6.18.1.3 *Defining the new test version*

This procedure is used to define the new test software release.

- Click the **Software management** menu.
- Select the **53xxip** range.
- Click **Change**.
- Click the link **Configure test software release**:
  - select terminal software package **R6.1_53xxip_E3_00** then click **Validate**.

**Note : The new terminal software R6.1_53xxip_E3_00 package is now the test release.**

#### 6.18.1.4 *Starting the update of the new test version*

- Click **Return**.
- A new window opens.

  This indicates the criteria concerned by the update of the new software release:
  - The **terminal range**: **53xxip**
  - The **Production software release**concerned: **R6.1_53xxip_E2_00**
  - The **Test software release**concerned: **R6.1_53xxip_E3_00**
- Enter the **Action name**.
- Select the test **Software release** concerned: **R6.1_53xxip_E3_00**
- Select the list to use in test mode: **test**
  - The **List details** link is used to display the terminals contained on the selected list.
- Select the **Type of update**:
  - Immediate
  - Deferred: specifies the date in DD/MM/YYYY format and time in HHMM format.

**Note : Clicking the icon opens the calendar so the date can be selected directly.**

- Click **Validate** to start updating the software release of all MiVoice 5300 IP Phones.

#### 6.18.1.5 *Checking that the test software release update is working correctly*

This operation is used to ensure that the new test software release has been correctly updated.

Refer to Chapter 6.16.1.5 for more information about the procedure.

### 6.18.2 DISTRIBUTING THE NEW TEST SOFTWARE RELEASE PARAMETERS

See Chapter 6.17.5 for how to define the distribution of the new test software release parameters.

### 6.18.3 UPDATING THE GLOBAL DATA OF THE TERMINALS USED WITH THE TEST SOFTWARE

This procedure is used to update the global data of MiVoice 5300 IP Phone in the test software release.

See Chapter 6.16.3 for details of the procedure, and use the following parameters:

- Select the **53xxip** range.
- In the field **Version to configure**, select the test release concerned by the global data update (**R6.1_53xxip_E3_00** in the example).

#### *6.18.3.1 Checking that the global data update process is working correctly in test mode*

This operation is used to ensure that the global data update in test mode has been performed correctly.

Refer to Chapter 6.16.3.1 for more information about the procedure.

### 6.18.4 UPDATING THE SPECIFIC DATA OF TERMINALS USED WITH THE TEST SOFTWARE

This procedure is used to update the specific data of MiVoice 5300 IP Phone in the test software release.

#### *6.18.4.1 Updating the specific data common to all terminals used with the test software*

This procedure is used to update the specific data of terminals in the test software release.

See Chapter 6.16.4.1 for details of the procedure, and use the following parameters:

- Select range **53xxip**.
- In the field **Version to configure**, select the test version concerned by the specific data update. (**R6.1_53xxip_E3_00** in the example).

#### *6.18.4.2 Updating the specific data of individual terminals used with the test software*

This procedure is used to update the special specific data of terminals in the test software release.

See Chapter 6.16.4.2 for details of the procedure, and use the following parameters:

- Select range **53xxip**.
- In the field **Version to configure**, select the test version concerned by the specific data update. (**R6.1_53xxip_E3_00** in the example).

### 6.18.5 CHECKING THAT THE UPDATE PROCESS IS WORKING CORRECTLY FOR SPECIFIC DATA IN TEST MODE

This operation is used to ensure that the specific data update in test mode has been performed correctly.

Refer to Chapter 6.16.4.3 for more information about the procedure.

### 6.18.6 EXITING THE TEST MODE

This procedure is used to leave the test mode at the end of the test phase.

Two possibilities are available:

- The tested new software release is satisfactory:  in this case, all the terminals on the installation must be updated with the new test software.

- The tested new software release is not satisfactory:  in this case, only the tested terminals must be updated with the current production software.

#### 6.18.6.1 Switching from test mode to production mode

In this case, the test software release must be defined as the new production software release, and an update operation for this new production software release started on all the terminals.

In the example below the initial situation is as follows:

- Production release = **R6.1_53xxip_E2_00**
- Test release = **R5.3_53xxip_A6_00**

- Click the **Software management** menu.
- Select the **53xxip** range.
- Click **Change**.
- Click the link **Configure production software release**:
  - Select release **R6.1_53xxip_E3_00**  and click **Validate**.

  the situation is now:
  - Production release = **R6.1_53xxip_E3_00**
  - No test version defined.
- Click **Return**.
- A new window opens.

  This indicates the criteria concerned by the update of the new software release:
  - The **terminal range**: **53xxip**
  - The **Production software release** concerned: **R6.1_53xxip_E3_00**
- Enter the **Action name**.
- Select the **Software release** concerned: **R6.1_53xxip_E3_00**
- Select the **Type of update**:
  - Immediate
  - Deferred: specifies the date in DD/MM/YYYY format and time in HHMM format.

**Note : Clicking the icon opens the calendar so the date can be selected directly.**

- Click **Validate** to start updating the production software release of all MiVoice 5300 IP Phones.

### 6.18.6.2 *Returning to the current version*

In this case, the test software release is not satisfactory. The terminals on the test list must be downgraded with the current production release. An update for this production software release must be started on all the terminals.

In the example below the initial situation is as follows:

- Production release = **R6.1_53xxip_E2_00**
- Test release = **R5.3_53xxip_A6_00**

- Click the **Software management** menu.
- Select the **53xxip** range.
- Enter the **Action name**.
- Select the **Software release** concerned: **R6.1_53xxip_E2_00**
- Select the **Type of update**:
  - Immediate
  - Deferred: specifies the date in DD/MM/YYYY format and time in HHMM format.



**Note : Clicking the icon opens the calendar so the date can be selected directly.**

- Click **Validate** to start updating the current production software release of all MiVoice 5300 IP Phones.



**Note : Only the terminals with the test software release will be updated with the current production software release because all the other terminals are already in the right version.**

# 6.19 MANAGING MIVOICE 5300 DIGITAL PHONES (TDM)

For TDM MiVoice 5300 Digital Phone, TMA offers the following functions:

- Inventory
- Updating terminal software (production release and test release)
- Actions display.

## 6.19.1 INVENTORY OF MIVOICE 5300 DIGITAL PHONES

TMA gives the configuration inventory of MiVoice 5300 Digital Phone, after first deployment.

The main data associated with a MiVoice 5300 Digital Phone are:

- directory number
- The terminal range and model
- Terminal software release
- The terminal site membership number
- The physical location on which the subscription is declared, and the terminal connected (cabinet, card, trunk).

The other fields do not concern this environment.

**Note : In R5.3 and later, if a MiVoice 5300 Digital Phone is inaccessible (card out of service) or is parked, the inventory associated with this terminal is refreshed. The previous physical location, as well as its type, is stored.**

To display the inventory of MiVoice 5300 Digital Phone configuration in TMA, proceed as follows:

- Click the **Inventory** menu.
- Select the **53xx** range and possibly the **Model**.

Information display depends on the filter used. This filter is activated by clicking the icon. 

- If possible, apply a filter to the current inventory based on:
  - The terminal subscription number
  - The terminal software release (production, test release, etc.)

**Note : The joker * may be applied to the Number parameters by placing it at the end of the parameter value.**

- Click**Filter** to apply the filter to the current inventory.

The version of the terminals in the **Software release** column is green in colour if it is the same as the terminal software release defined as the production software release.

## 6.19.2 MANAGING THE LIST OF TERMINALS FOR MIVOICE 5300 DIGITAL PHONES

This procedure is used to define a list of terminals for all models of MiVoice 5300 Digital Phones.

This list is used in test mode to upgrade the software release of terminals over a limited range.

**ATTENTION : In test mode, the list contains a maximum of 10 terminals.**

**ATTENTION : A terminal may be assigned only to one list at a time.**

### *6.19.2.1 Defining a new list by entering the terminals one by one*

- Click the **Inventory** menu.
- Select the **53xx** range and possibly the **Model**.
- Click **List management:**

  A new window opens. This window gives the criteria concerned by the list creation:

  - The **terminal range**: **53xx**
  - The Telephone set **model** concerned
- Click **Add new list**.

  A new window opens. This window allows you to enter one by one the terminals contained on the list.
- In the right input area, for each terminal to be added to the list, enter the directory number of the terminal then click **Add set**.

**Note : To delete a terminal from the currently edited list, select the terminal then click Delete.**

- In the right area, enter the **List name** then click **Confirm**.
  - The message has been successfully saved.
- Close the window either by clicking the **Close window** link, or by clicking on the top right side of the window.
- The list management window is refreshed and then displays:
  - The list name
  - The number of terminals contained on the list
  - The **Action** field used to delete or modify the displayed list.
- Click **Return** to return to the **Inventory** window.

### *6.19.2.2 Modifying a list*

- Click the **Inventory** menu.
- Select the **53xx** range and possibly the **Model**.
- Click **List management:**

  A new window opens. This window gives the criteria concerned by the list creation:

  - The **terminal range**: **53xx**
  - The Telephone set **model** concerned

- In the **Action** field, click the icon of the list to modify.
- Modify the list by adding or deleting a terminal.
- Click **Confirm**.
  - The message has been successfully saved.
- Close the window either by clicking the **Close window** link, or by clicking on the top right side of the window.
- The list management window is refreshed and then displays:
  - The list name
  - The new number of terminals contained on the list
- Click **Return** to return to the **Inventory** window.

#### *6.19.2.3 Deleting a list*

- Click the **Inventory** menu.
- Select the **53xx** range and possibly the **Model**.
- Click **List management:**

  A new window opens. This window gives the criteria concerned by the list creation:
  - The **terminal range**: **53xx**
  - The Telephone set **model** concerned
- In the **Action** field, click the icon of the list to delete:
  - a confirmation message is displayed so you can confirm or cancel the list deletion.
- The list management window is refreshed and the deleted list no longer appears.
- Click **Return** to return to the **Inventory** window.

## 6.19.3 UPDATING THE TERMINAL SOFTWARE RELEASE OF MIVOICE 5300 DIGITAL PHONES

This procedure is used to update the software release of all MiVoice 5300 Digital Phones known to the inventory.

**Note : In R5.3 and later, during each MiVoice 5300 Digital Phone update operation (software), TMA checks the accessibility of the sites concerned by the action. In case of error during this check, the action is not performed.**

### *6.19.3.1 Installing the new software release to be deployed*

Refer to section 6.15.4.1

### *6.19.3.2 Defining the new production release*

This procedure is used to define the new production software release.

Refer to the previous figure then

- Click the **Software management** menu.
- Select the **53xx** range.
- Click **Change**.
- Click the link **Configure production software release**:
  - Select the new production release and click **Validate**.

**Note : The new software release is now the production release and all the terminals appear in red in the inventory (terminals seen in another software release).**

### *6.19.3.3 Starting the update of the new production release*

- Click **Return**.
- A new window opens.

  This indicates the criteria concerned by the update of the new software release:
  - The **terminal range**: **53xx**
  - The **Production software release**concerned
- Enter the **Action name**.
- Select the **Software release** concerned.
- Select the **Type of update**:
  - Immediate
  - Deferred: specifies the date in DD/MM/YYYY format and time in HHMM format.

**Note : Clicking the icon opens the calendar so the date can be selected directly.**

- Click **Validate** to start updating the software release of all MiVoice 5300 Digital Phones.

## 6.19.4 CHECKING THAT THE UPDATE PROCESS IS WORKING CORRECTLY FOR THE PRODUCTION SOFTWARE RELEASE

This operation is used to ensure that the new software release has been correctly updated.

- Click the **Action monitoring** menu.

- Check in **Action monitoring,** the status of the production release update operation:
  - If the operation was successful, the status indicates: **Success**
- Click the  icon to view the progress of the on-going production release update operation.
  - A colour code is used to check whether the terminals have the expected software release (green colour) or not (red colour). This colour code is only significant for the last action of this type. The information displayed may or may not be filtered with this criterion.
- Check in the **Event log** the status of the terminal software release update operation.
  - If the operation was successful, the status indicates: **Action successful. Action on MiVoice 5000 PBX taken into account.**

The number of transferred files is used to check that all new software release files have actually been placed in the storage directory of the FTP server used for day-to-day terminal management. The system concerned by the action is also indicated.

# 6.20 TEST MODE FOR MIVOICE 5300 DIGITAL PHONES

The test mode is used to update the terminals' software release, global data and specific data on a range limited to 10 terminals maximum. This function is used to test a new terminal software application or new function/configuration on a small number of terminals before exposing it to all the terminals.

## 6.20.1 UPDATING MIVOICE 5300 DIGITAL PHONE SOFTWARE RELEASE IN TEST MODE

This procedure applies once a terminal appears in the TMA application inventory. This procedure is used to update the software release of the MiVoice 5300 Digital Phones known to the inventory and defined on a list containing at most 10 terminals.

In the example below:

- The production release = **R6.1_53xx_A2_00**
- The test release = **R6.1_53xx_A3_00**

**ATTENTION : In test mode, only one software release update operation can be performed at a time for a list of terminals.**

### *6.20.1.1 Defining a test list*

See Section 6.19.2 for how to define a list of terminals containing a maximum of 10 terminals.

This list, called **test** , will be used in the procedure described below.

**ATTENTION : A list used by an on-going test cannot be deleted or modified.**

### *6.20.1.2 Installing the new test software release*

Refer to section 6.15.4.1

### *6.20.1.3 Defining the new test version*

This procedure is used to define the new test software release.

- Click the **Software management** menu.
- Select the **53xx** range.
- Click **Change**.
- Click the link **Configure test software release**:
  - Select the test terminal software package **R6.1_53xx_A3_00** then click **Validate**.

**Note : The new terminal software R6.1_53xx_A3_00 package is now the test version.**

## 6.20.2 STARTING THE UPDATE OF THE NEW TEST VERSION

- Click **Return**.
- A new window opens.

  This indicates the criteria concerned by the update of the new software release:
  - The **terminal range**: **53xx**
  - The **Production software release** concerned: **R6.1_53xx_A2_00**

- The **Test software release**concerned: **R6.1_53xx_A3_00**

- Enter the **Action name**.
- Select the test **Software release** concerned: **R6.1_53xx_A3_00**
- Select the list to use in test mode: **test**
  - The **List details** link is used to display the terminals contained on the selected list.
- Select the **Type of update**:
  - Immediate
  - Deferred: specifies the date in DD/MM/YYYY format and time in HHMM format.

**Note :** **Clicking the icon opens the calendar so the date can be selected directly.**

- Click **Validate** to start updating the software release of all MiVoice 5300 Digital Phones.

### 6.20.3 CHECKING THAT THE TEST SOFTWARE RELEASE UPDATE IS WORKING CORRECTLY

This operation is used to ensure that the new test software release has been correctly updated.

- Click the **Action monitoring** menu.
- Check in **Action monitoring,** the status of the test version update operation: if the operation is successful, the status displays: **Success**
- Click the  icon to view the progress of the on-going test software release update operation.
  - A colour code is used to check whether the terminals have the expected software release (green colour) or not (red colour). This colour code is only significant for the last action of this type. The information displayed may or may not be filtered with this criterion.
  - The **List** field displays the list used in test mode: **test**
  - The **Test** field is used to check whether or not the on-going operation is in test mode.
- Check in the **Event log** the status of the test software release update operation.
  - If the operation was successful, the status indicates: **Action successful. Action on MiVoice 5000 PBX taken into account.**

The number of transferred files is used to check that all new test software release files have actually been placed in the test storage directory of the FTP server used for day-to-day terminal management in test mode.

### 6.20.4 EXITING THE TEST MODE

This procedure is used to leave the test mode at the end of the test phase.

Two possibilities are available:

- The tested new software release is satisfactory: in this case, all the terminals on the installation must be updated with the new test software.
- The tested new software release is not satisfactory: in this case, only the tested terminals must be updated with the current production software.

#### *6.20.4.1 Switching from test mode to production mode*

In this case, the test software release must be defined as the new production software release, and an update operation for this new production software release started on all the terminals.
In the example below the initial situation is as follows:

  - Production release = **R6.1_53xx_A2_00**
  - Test release = **R6.1_53xx_A3_00**
- Click the **Software management** menu.
- Select the **53xx** range.
- Click **Change**.
- Click the link **Configure production software release**:
  - Select release **R6.1_53xx_A3_00** and click **Validate**.

  The situation is now:
  - Production release = **R6.1_53xx_A3_00**
  - No test version defined.
- Click **Return**.
- A new window opens.

This indicates the criteria concerned by the update of the new software release:

- The **terminal range**: **53xx**
- The **Production software release** concerned: **R6.1_53xx_A3_00**

- Enter the **Action name**.
- Select the **Software release** concerned: **R6.1_53xx_A3_00**
- Select the **Type of update**:
  - Immediate
  - Deferred: specify the date in DD/MM/YYYY format and time in HHMM format.

**Note : Clicking the icon opens the calendar so the date can be selected directly.**

- Click **Validate** to start updating the production software release of all MiVoice 5300 Digital Phones.

### *6.20.4.2 Returning to the current version*

In this case, the test software release is not satisfactory. The terminals on the test list must be downgraded with the current production release. An update for this production software release must be started on all the terminals.

In the example below the initial situation is as follows:

- Production release = **R6.1_53xx_A2_00**
- Test release = **R6.1_53xx_A2_00**

- Click the **Software management** menu.
- Select the **53xx** range.
- Enter the **Action name**.
- Select the **Software release** concerned: **R6.1_53xx_A2_00**
- Select the **Type of update**:
  - Immediate
  - Deferred: specifies the date in DD/MM/YYYY format and time in HHMM format.

**Note : Clicking the icon opens the calendar so the date can be selected directly.**

- Click **Validate** to start updating the current production software release of all MiVoice 5300 Digital Phones.

**Note : Only the terminals with the test software release will be updated with the current production software release because all the other terminals are already in the right version.**

# 6.21 ADDITIONAL TMA FUNCTIONS

## 6.21.1 DOWNLOADING FILES INDIVIDUALLY

As of R6.1 SP1, a new feature is used to download an individual file to the FTP server(s). This feature is used, in particular, to provide on the FTP server(s) with the template files (Mitel 6000 SIP Phone.cfg) used by Mitel 6000 SIP Phones and the certificates (ca.crt) used by Mitel 6000 SIP Phones and MiVoice 5300 IP Phones when encryption is enabled and an external certificate is used.

To download a file individually, proceed as follows:

- Click the **Deployment** menu.
- Select the range (**6xxxi or 53xxip)** .
- From the **List of FTP servers,** select the FTP server to which the certificate must be downloaded.
- In the **Other file** field import, by clicking **Browse**, the template file (Mitel 6000 SIP Phone.cfg) or certificate (ca.crt) to download.
- Click **Validate**.
- Enter the **Action name**.
- Indicate **the type of update**: immediate or deferred.
- Click **Validate**.
- In **Action monitoring** check that the file is correctly downloaded individually to the FTP server.



**ATTENTION : An FTP server must be selected. Only one file is authorised per provisioning operation. This file is not backed up in the TMA directories.**



**ATTENTION : Some file name checks are made:**

- **This cannot be a global data file; therefore, the name must be different from aastra.cfg (if 6xxxi range is selected) or localdb.config.ftp (if 53xxip range is selected).**
- **If configuration file encryption is activated, TMA does not allow *.cfg files to be sent to the FTP server as they will not be taken into account.**
  **In release R2.1 and above, this check is no longer made.**



**ATTENTION : The terminal must be restarted for the template file or certificate to be taken into account.**

### 6.21.2 EXPORTING THE DATA CONTAINED IN THE MITEL 6000 SIP PHONE AND MIVOICE 5300 IP PHONE CONFIGURATION FILES

**ATTENTION : This feature only applies to Mitel 6000 SIP Phone and MiVoice 5300 IP Phone.**

The global and specific data of terminals with a production or test software release may be exported in **.csv** format from the **Terminals configuration export** menu.

- Click the **Terminal configuration export** menu.
- Select the **range** and possibly the **model**.

To export the data of terminals with the production software release:

- Click **Prod data**.
- Click the **global data file** link to export the global data of terminals with the production software release.
- Click **Save** to back up the file **export_global.csv**.
- Click **Save** again after selecting the target directory.
- Click the **specific data file** link to export the specific data of terminals with the production software release.
- Click **Save** to back up the file **export_specific.csv**.
- Click **Save** again after selecting the target directory.

To export the data of terminals with the test software release:

- Click **Test data**.

Then proceed as described above to save the export files.

### 6.21.3 EXPORTING THE DATA CONTAINED IN THE INVENTORIES OF MITEL 6000 SIP PHONE, MIVOICE 5300 IP PHONE AND MIVOICE 5300 DIGITAL PHONE

Export is only possible on the terminals available in the inventory. A filter can be applied before exporting the data.

- Click the **Inventory** menu.
- Select the **range** and possibly the **model**.
- Information about each terminal saved on its reference site is displayed.
  - The terminals associated with a production software release appear in green in the **Software version** column.
  - The terminals associated with a test software release appear in orange in the **Software version** column.
  - The terminals associated with any other software release appear in red in the **Software version** column.
  - Information display depends on the filter used. This filter is activated by clicking the icon. 
- If possible, apply a filter to the current inventory based on:
  - The terminal subscription number
  - The terminal IP address
  - The terminal software release (production, test release, etc.)
  - The terminal global data index

- The terminal specific data index
- The terminal MAC address
- Terminal encryption configuration:
  - SRTP (and TLS) mode activated (terminals 53xxip and 6xxxi)
  - TLS mode activated (terminals 6xxxi)
  - No encryption activated.

**Note : The joker * may be applied to the parameters Number, IP address and Mac address by placing them at the end of the parameter value.**

- Click**Filter** to apply the filter to the current inventory.
- Click the  icon to start exporting the data available in the inventory.
- Click **Save** to save the file as **journal.csv**.
- Click **Save** again after selecting the target directory.

**Note : The export function is also available from Action monitoring.**

### 6.21.4 PRINTING OUT THE DATA CONTAINED IN THE INVENTORIES OF MITEL 6000 SIP PHONE, MIVOICE 5300 IP PHONE AND MIVOICE 5300 DIGITAL PHONE

The terminal data displayed in the inventory can be printed out. A filter can be applied before printing the data.

See Chapter 6.21.3 for how to select the terminals displayed in the inventory.

- Click the  icon to start printing the data available in the inventory.
- The data can be previewed in a window before being printed.
- Click **Print** to start printing the data.

**Note : The print function is also available from Action monitoring.**

### 6.21.5 EVENTS LOG

The event log is basically used to check the status of the following actions:

- Deployment
- Terminal software release update
- Terminal global data update
- Terminal specific data update

Each action is identified by the following information:

- The **Date** on which the action was started
- The **Time** the action was started
- The name of the **User** who started the action
- The type of**Action** concerned
- The **Name of the action** concerned
- The **Status** of the action concerned

The information displayed may be filtered with certain criteria:

- Click the **Event log** menu.
- Select any of the following:
  - **User**
  - **Action**
  - **Status**
  - **Start date** and **End date.**

**Note : Clicking the icon opens the calendar so the start and end dates can be selected directly.**

- Click **Filter** for the filtering criteria to become effective.

**Note : Clicking Initialise deletes the filter criteria and displays the entire information.**

In case of operation error, the events log is used to identify the cause of the error: The following cases are taken into account:

- Network problem: no response to PING (problem accessing the MiVoice 5000 PBX),
- APACHE problem: HTTPS request timed out (problem accessing the MiVoice 5000 PBX web server),
- "MMC" service is stopped (problem accessing the MiVoice 5000 PBX MMC),
- Incorrect "login/password" (problem authenticating to the MiVoice 5000 PBX),
- Problem while sending the ".csv" file (problem sending files to the MiVoice 5000 PBX),
- Errors while sending the terminal update request: error codes are logged, but the error is not interpreted (MMC request problem (error code xx) on the MiVoice 5000 PBX).

### 6.21.6 DELETING A SOFTWARE RELEASE

This function deletes a software release installed in TMA.

The deletion is only possible if the software release is not configured as the production or test software release.

Proceed as follows:

- Click the **Software management** menu.
- Select the range.
- Click **Change**.
- Click the link **Delete a software version**:
  - select the version to delete then click **Confirm**.

The selected software release is deleted from TMA.

**Note : The selected software release is not deleted by TMA from the external FTP server storage directory. This operation must be performed manually on the external FTP server.**

# 6.22 PROGRAMMING SYSTEM KEYS FOR MITEL 6000 SIP PHONES (TEMPLATE MANAGEMENT)

**ATTENTION : As of R6.2, the Templates management menu has been replaced with the Deployment menu.**

The keys of Mitel 6000 SIP Phones are divided into two categories: system keys and programmable keys.

In addition to the configuration of terminal Mitel 6000 SIP Phone keys, possible on Web Admin **Menu Telephony service > Subscribers > Terminals and Applications > 6xxxi keys**, TMA completes the possibilities to program the **System** keys (speed-dial for example).

The programming for these **System** keys will be generally applied by terminal model:

- 6863 SIP,
- 6865 SIP
- 6867 SIP,
- 6869 SIP,
- 6873 SIP,
- 6710 SIP,
- 6730 SIP,
- 6731 SIP,
- 6735 SIP,
- 6737 SIP,
- 6739 SIP,
- 6753 SIP,
- 6755 SIP,
- 6757 SIP

**Note : This type of programming is not applicable to terminal 6751 SIP (no programmable key on this model).**

The programming for these **System** keys must be indicated, for each terminal model, in a specific pre-formatted file called "**TEMPLATE**". These files are available in the **sip_sets_tma** directory of the MiVoice 5000 software R6.2 CD-ROM.

**Procedure:**

- Create the file from the model provided and save it respecting the **67xxi.cfg** syntax (example 6755i.cfg).
- From the **Templates management** menu, successively download all the "**Templates**" files concerned.

After the template is downloaded, the specific data file is created based on the MAC address **@mac.cfg** or it is updated, if already available, by TMA:

- For a new terminal, during first connection (first REGISTER), the specific file is automatically generated, and the keys of the terminal in question programmed after the terminal is started.
- For already connected, working terminals, specific data update must be run manually(see Section 6.15.3).

**Note : As from R6.1 SP1 it is possible, via the Deployment menu, to download into the FTP server storage area a template file (6xxxi.cfg) using the parameter Other file.**

**ATTENTION : The terminal must be restarted for the template file or certificate to be taken into account.**

## 6.23 DEPLOYING AND CONFIGURING NEW MITEL 6000 SIP PHONES IN A WORKING INSTALLATION

This procedure describes the step to take in order to deploy and re-configure Mitel 6000 SIP Phone in a working installation.

We consider that TMA has been correctly configured for already deployed and working terminals Mitel 6000 SIP Phones:

- The integrated FTP server has been configured with the right accounts.
- A production release has been defined.
- All the terminals are in the production release.
- The terminal inventory is up to date.
- The distribution of parameters has been defined for the production release.
- The global and specific configuration files have been defined in TMA for the production release.
- The integrated FTP server storage directory, used for day-to-day terminal management, contains the production software release as well as the global and specific data configuration files.

### 6.23.1 DEPLOYING NEW MITEL 6000 SIP PHONES AUTOMATICALLY

To automatically deploy new Mitel 6000 SIP Phone, refer to Chapter 6.8.1 or 6.8.1 .

### 6.23.2 CHECKING THE DEPLOYMENT OF MITEL 6000 SIP PHONES

See Chapter 6.8.5 for how to check that the deployment of new terminals via manual login has been completed correctly.

### 6.23.3 DAY-TO-DAY MANAGEMENT OF THESE NEW MITEL 6000 SIP PHONES

See Chapter 6.10 for the day-to-day management of these new Mitel 6000 SIP Phones.

## 6.24 DEPLOYING AND CONFIGURING NEW MIVOICE 5300 IP PHONES IN A WORKING INSTALLATION

This procedure describes the step to take in order to deploy and re-configure MiVoice 5300 IP Phones in a working installation.

We consider that TMA has been correctly configured for already deployed and working terminals MiVoice 5300 IP Phones:

- The integrated FTP server has been configured with the right accounts.
- A production release has been defined.
- All the terminals are in the production release.
- The terminal inventory is up to date.
- The distribution of parameters has been defined for the production release.
- The global and specific configuration files have been defined in TMA for the production release.
- The integrated FTP server storage directory, used for day-to-day terminal management, contains the production software release as well as the global and specific data configuration files.

### 6.24.1 DEPLOYING NEW MIVOICE 5300 IP PHONES AUTOMATICALLY

To automatically deploy new MiVoice 5300 IP Phones, refer to Chapter 6.9.1 .

### 6.24.2 CHECKING THE DEPLOYMENT OF MIVOICE 5300 IP PHONES

See Chapter 6.9.3 for how to check that the deployment of new terminals via manual login has been completed correctly.

### 6.24.3 DAY-TO-DAY MANAGEMENT OF THESE NEW MIVOICE 5300 IP PHONES

See Chapter 6.17 for the day-to-day management of these new MiVoice 5300 IP Phones.

## 6.25 AUTOMATICALLY DEPLOYING AND UPDATING MIVOICE 5300 IP PHONE AND MITEL 6000 SIP PHONES WHILE UPGRADING A MIVOICE 5000 SYSTEM

The integrated TMA allows the deployment and automatic update of MiVoice 5300 IP Phones and Mitel 6000 SIP Phones while updating a MiVoice system in a simplified network architecture, using the integrated FTP and DHCP servers.



**ATTENTION : This procedure only applies if:**

- **the software release of the MiVoice 5300 IP Phones and Mitel 6000 SIP Phones contained in the terminal software package available in the new MiVoice 5000 system release is ≥ the production software release configured in the integrated TMA,**
- **If the integrated FTP and TMA services are enabled.**



**ATTENTION : See the document AMT/PTD/PBX/0151* for a detailed description of the upgrade procedures.**

### 6.25.1 PRINCIPLE

The following operations are performed automatically when the Mitel 5000 Gateways software is upgraded from R6.1 to R6.2:

- The integrated TMA application is automatically configured with the integrated FTP server.
- The production software release of the integrated TMA is automatically configured with the new software releases of Mitel 6000 SIP Phones and MiVoice 5300 IP Phones, contained in the new MiVoice 5000 R6.2.
- The software releases of Mitel 6000 SIP Phone and MiVoice 5300 IP Phone, contained in the new release R5000 R6.2, are moved to the work directories of the integrated TMA (the new version of Mitel 6000 SIP Phones is also available in the deployment directory: **deployment_67xxi** via some symbolic links).
- The global data configuration file of Mitel 6000 SIP Phone and MiVoice 5300 IP Phone is generated:
  - From the parameters contained in the global data configuration file in the old release R6.1 and the new, mandatory global parameters contained in the new release R6.2,
- The global data configuration file used to deploy Mitel 6000 SIP Phones is automatically updated with the operation information.
- Some automatic actions are automatically started by the integrated TMA to update the new software releases and global data configuration file of MiVoice 5300 IP phones and Mitel 6000 SIP phones.
- If some specific files are used in for Mitel 6000 SIP Phone and/or MiVoice 5300 IP Phone (MAC@.cfg and/or locadb.config.MAC@.ftp), these files are kept after upgrading to R6.2 and are still located both in the new storage directories used by these terminals and in the work directories of TMA.

### 6.25.2 UPGRADING A MIVOICE 5000 SYSTEM

See the document AMT/PTD/PBX/0151* for a detailed description of the upgrade procedures.

### 6.25.3 AUTOMATIC UPDATE OF MITEL 6000 SIP PHONES AND MIVOICE 5300 IP PHONES

After MitVoice 5000 System started, some automatic actions are automatically started by the integrated TMA to update the new software releases and global data configuration file of MiVoice 5300 IP Phone and Mitel 6000 SIP Phones (respectively the files localdb.config.ftp and aastra.cfg).

During the first REGISTER transmitted by MiVoice 5300 IP phones and Mitel 6000 SIP Phones already assigned to a subscription, a request to update the terminals' software and global data configuration file is sent by Mitel 5000 Gateways to these terminals.

MiVoice 5300 IP Phones and Mitel 6000 SIP Phones restart automatically to take account of the new terminal software releases defined as production software release in the integrated TMA and the new global data configuration file updated automatically during upgrade from the parameters contained in the global data configuration file of the old release and the new, mandatory global parameters contained in the new release.

### 6.25.4 DEPLOYING NEW MIVOICE 5300 IP PHONES AUTOMATICALLY

To deploy new MiVoice 5300 IP Phones, refer to Chapter 6.9.1 .

### 6.25.5 DEPLOYING NEW MITEL 6000 SIP PHONES AUTOMATICALLY

To deploy new Mitel 6000 SIP Phone, refer to Chapter 6.8.1 or 6.8.1 .

### 6.25.6 CHECKING THE DEPLOYMENT OF MIVOICE 5300 IP PHONES AND MITEL 6000 SIP PHONES

See Chapter 6.9.3 to check that the automatic update of Mitel 6000 SIP Phones and MiVoice 5300 IP Phones has taken place correctly, as well as the deployment of the new terminals via manual login.

## 6.26 UPDATING MIVOICE 5300 DIGITAL PHONE SOFTWARE RELEASE WHILE UPGRADING A MIVOICE 5000 SYSTEM

This procedure is used to update the software release of all MiVoice 5300 Digital phones connected physically to the Mitel 5000 Gateways on some equipment and subscriptions in service while upgrading A MiVoice 5000 System.

***This procedure applies only in the following cases:***

- ***If the software release of the MiVoice 5300 Digital Phones contained in the new software release is ≥ in the production software release defined in the integrated TMA.***

The following operations are performed during the upgrade:

- The production software release of the integrated TMA is automatically configured with the new software release of MiVoice 5300 Digital Phones, contained in MiVoice 5000
- The software release of MiVoice 5300 Digital phones, contained in release R5000 , is moved to the work directory of the integrated TMA.

### 6.26.1 UPDATING MIVOICE DIGITAL PHONES VIA THE INTEGRATED TMA

Refer to Chapter 6.19.3 .

### 6.26.2 STARTING THE UPDATE OF THE NEW PRODUCTION RELEASE

Refer to Chapter 6.15.4.3 .

### 6.26.3 CHECKING THE MIVOICE 5300 DIGITAL PHONE UPDATE

Refer to Chapter 6.15.4.4 .

# 7 MANAGING TERMINALS WITH TMA HOSTED BY MIVOICE 5000 MANAGER

## 7.1 PRESENTATION AND PRINCIPLES

The TMA (**T**erminal **M**anagement **A**pplication) is used to deploy and update the following terminals:

- MiVoice 5300 IP phones,
- Mitel 6000 SIP Phones,
- MiVoice 5300 Digital Phones (TDM).

TMA may be integrated into a Mitel 5000 Gateways system (accessible from Web Admin) or centralised on a MiVoice 5000 Manager as of release 2.1C.

This chapter is devoted to the TMA on MiVoice 5000 Manager.



**Note : For information on management from the TMA integrated into MiVoice 5000 (Mitel 5000 Gateways or Mitel 500 Server), see Chapter 6.**

***The TMA service must be deactivated on the iPBX when the TMA of MiVoice 5000 Manager is used.***

No special additional licence is required to use TMA. However, the "Subscriber management" licence must be unlocked in MiVoice 5000 Manager to access the TMA start menu.

The main actions on the terminals, based on the range, are described in Chapter 5.



**Note : During each terminal update operation (software, configuration), TMA checks the accessibility of the sites and external FTP servers concerned by the action. In case of error during this check, the action is not performed.**

## 7.2 LAUNCHING THE TMA

- Start TMA from the MiVoice 5000 Manager Client application on a Windows client PC:
  - Click the **Telephony** menu then the **Terminal management** menu.
  - For a configuration with several multi-site architectures, a new window opens: select the region, multi-site/isolated site then click **Continue**.

Enter the login and password assigned by the administrator: the TMA welcome window opens.

The following menus are accessible in the left column:

- **Call Dist**: This menu is used to return to the Web Admin home page.
- **Application configuration**: This menu is used to:
  - Cancel the management of global and specific data files and to retain only software update actions on the terminals, in the actions managed by TMA
  - Activate the configuration file encryption mode
  - Activate or deactivate TMA-EP mode
  - Activate the Remote Worker feature
  - Exclude one or more sites: the sites concerned are no longer managed by TMA.
  - Test the accessibility of the FTP servers and sites before starting an action.
- **Model management**: This menu is used toavtivate or not the management of selected models

- **Servers configuration**: This menu is used to define the parameters of the external storage FTP server(s).
- **Inventory**: This menu is used to view the inventory of installation terminals and manage the list of terminals.
- **Software management**: This menu is used to install and manage the terminal software releases and start terminal update actions.
- **Templates management**: This menu is used to complete the programming possibilities of **System** keys on Mitel 6000 SIP Phones for those that can be performed from Web Admin.
- **Terminals configuration**: This menu is used to distribute the global and specific parameters and to start data update on the terminal.
- **Deployment**: Deployment: this menu is used to manually deploy the terminals. This menu is also used to make available to the FTP server(s) the template files (modele.cfg) used by Mitel 6000 SIP Phones and the certificates (ca.crt) used by Mitel 6000 SIP Phones and MiVoice 5300 IP Phones.
- **Terminals configuration export**: This menu is used to export in **.csv** format the global and specific data about Mitel 6000 SIP Phones and MiVoice 5300 IP Phones.
- **Actions display**: This menu is used to display the actions started on the terminals (deployment, terminal software, global and specific data).
- **Events log**: This menu displays the events log.
- **iPBX configuration**:
- This menu is used to send a request to an iPBX in order to delete the TDW tables containing the data version and index information expected for the terminals. This menu must be used after a TMA /TMA-EP passage. This function is only available for sites as of R5.2 SP1.
- This menu is also used to manage the integrated FTP server, i.e. to delete the content of the FTP areas on an iPBX (as of R6.3). This function can be useful if you wish to use an integrated FTP server in TMA in MiVoice 5000 Manager.

# 7.3 CONFIGURING THE TMA APPLICATION

## 7.3.1 ACTIVATING AND DEACTIVATING TMA-EP MODE

See TMA-EP operating manual (AMT/PTD/TR/0027*)

## 7.3.2 CONFIGURING THE TERMINALS

Refer to Chapter 6.3.1 à la page 103.

**Note : The management of Mitel 6000 SIP Phone and MiVoice 5300 IP Phone configuration files concerns all the multi-sites and sites managed by MiVoice 5000 Manager.**

## 7.3.3 ENCRYPTING CONFIGURATION FILES

Refer to Chapter 6.3.2 à la page 103.

**Note : The activation of configuration file encryption concerns all the multi-sites and sites managed by MiVoice 5000 Manager.**

## 7.3.4 ENABLING AND DISABLING REMOTE WORKER MANAGEMENT

See the document Remote Worker via MBG - AMT/PTD/PBX/0161 - for more information about the deployment of this function.

**Note : The remote worker management function concerns all the multi-site architectures and sites managed by MiVoice 5000 Manager.**

## 7.3.5 EXCLUDING ONE OR MORE SITES

The **Application configuration** menu is used to exclude one or more sites.

The sites concerned are no longer managed by TMA, with the following restrictions and impacts:

- The terminals of an "excluded" site always appear in the inventory.
- It is not possible to create a site-based list on this site. However, when a list is being created by entering numbers, the terminals of this site can always be added to a list.
- For FTP server configuration, excluded sites no longer appear on the list of available sites associated with an FTP server.
- If an FTP server is associated with "excluded" sites only, during (software or data) update, the update files will not be transferred to it.
- During a software or global data update, the tables of MiVoice 5000 systems concerned are not updated.
- During an action that requires the use of a list (software update in test mode, specific data update), if the list contains some terminals from "excluded" sites, this action is not authorised: an information message appears.
- Concerning automatic actions (MD5 + 1st LOGIN), if the notification concerns an "excluded" site, automatic specific data update is not performed.
- The menu used to exclude some sites is not accessible if some actions are programmed.

**ATTENTION : If an FTP server is associated with several sites, it will be updated during an action even if any of the associated sites is considered as "excluded". If any of the these sites is restarted, it will retrieve some data not compatible with the content of the site tables.**

To exclude one or more sites, select the **Application configuration** menu from the TMA main menu.

- Select the **Region and Multisite** concerned**.**
- Click **Sites under maintenance**.
- In the site exclusion window, tick the site(s) concerned then click **Save** to confirm.
- Close the window.

**Note : MiVoice 5300 Digital Phone, MiVoice 5300 IP Phone and Mitel 6000 SIP Phone are concerned by this function.**

### 7.3.6 TESTING THE CONFIGURATION

The **Application configuration** menu is used to check the site and FTP server accessibility before starting an action. The list of FTP servers and sites to be tested depends on the action configured by the administrator.

A new "TestConfig" action is available in the events log and gives the result of the configuration test.

To test the configuration, select the **Application configuration** menu from the TMA main menu.

- Select the **Region and Multisite** concerned**.**
- Click **Test configuration**.
- In the next window, select:
  - The terminal range concerned by the test: **53xxip** or **6xxxi** or **53xx**
  - The list concerned: **all** or a list defined by the administrator
  - The action name
- Click **Validate**.

**Note : MiVoice 5300 Digital Phone, MiVoice 5300 IP Phone and Mitel 6000 SIP Phone are concerned by this function.**

## 7.4 MODEL MANAGEMENT

Model management is carried out from this menu and is taken into account in the Embedded TMA.

When downloading a terminal package, Embedded TMA retains only software of the managed model s.

As a result, during a software update, only the files related to the managed models are sent to the FTP servers.

# 7.5 DEPLOY THE TERMINALS

## 7.5.1 PRINCIPLE

The TMA application is generally in charge of providing configuration software and files on one or more FTP servers, especially during deployment.

In a multi-site configuration, TMA is started from MiVoice 5000 Manager and the FTP servers must be manually defined in the Servers configuration menu.

The integrated TMA in MiVoice 5000 Manager requires the use of one or more external FTP servers:

- **For an external dedicated FTP server**, the integrated TMA in MiVoice 5000 Manager uses some FTP accounts to copy the files (configuration software and files) from the TMA application directories to the external FTP server directories.
- **For an external FTP server integrated into Mitel 5000 Gateways or MiVoice 5000 Server**, the TMA integrated into MiVoice 5000 Manager uses the accounts of the FTP server integrated into Mitel 5000 Gateways or MiVoice 5000 Server to copy the files (configuration software and files) from the TMA directories to the integrated FTP server directories.



**Note : Concerning the actual configuration of an external FTP server on Windows 2000/2003 server or MiVoice 5000, refer to Chapter 11.**



**Note : During each terminal update operation (software, configuration), TMA checks the accessibility of the sites and external FTP servers concerned by the action. In case of error during this check, the action is not performed.**

All the network parameters required by the terminal to work properly are from the DHCP server and the configuration files downloaded from the FTP server.

DHCP server configuration according to terminal type is described in Chapter 10.



**Note : The DHCP server may be hosted by a Windows 2000/2003 platform or by MiVoice Server.**

**On the iPBX side**

All the subscribers must be declared on the multi-site sites.

## 7.6 DEPLOYING MITEL 6000 SIP PHONES

Prerequisites:

- The DHCP and FTP servers are working.
- Subscriptions exist on each iPBX.

It is possible to log on Mitel 6000 SIP Phone via the MiVoice 5000 User Portal application. A new global 6xxxi parameter is used to open this feature. The user selects a terminal on which to log on via the MiVoice 5000 User Portal application from its system label. This label is unique and automatically generated by the Mitel 5000 Gateways system. This label can be modified individually or massively.

A global parameter can be configured to disable the free seating function. In this case (parameter unticked, the impact is as follows:

- On Mitel 6000 SIP Phones, the Ident key is no longer displayed, and manual login from the terminals is rejected for all the Mitel 6000 SIP Phones on the installation.

This parameter is accessible via Menu **Telephony service** > **Subscribers** > **Terminals and Applications** > **6xxxi parameters**, and is called **Manual login authorisation on any terminal type**. By default, this parameter is enabled (ticked). This parameter is accessible if login via MiVoice 5000 User Portal is open.

A new tool for deploying Mitel 6000 SIP Phones through automatic login is configurable by automatically assigning a directory number to each terminal identified by its unique label. Automatic login is carried out next time the terminal is registered. This tool concerns all the (secure and unsecured) subscriptions.

It is possible to secure or not the login tool during the Mitel 6000 SIP Phone deployment phase. A new subscription parameter is used to carry out this configuration:

- In non-secure mode, the parameter **Login via PC only** is not ticked (default value): the user can log on manually via the Ident key or via the corresponding feature code (*44 by default).
- In secure mode, the parameter **Login via PC only** is ticked: the user cannot log on manually via the Ident key or via the corresponding feature code (*44 by default).

It is possible to reinforce the security of the MiVoice 5000 User Portal access by configuring and using Single Sign-on (SSO) mode (see document AMT/PTD/PBX/0080* for how to configure SSO mode).

Mitel 6000 SIP Phones can be deployed using the following methods:

- Deployment through manual login on the terminal (**as of R5.2 only)**
- Deployment via MiVoice 5000 User Portal from a unique label identifying the terminal (**as of R6.2 only)**
- Automatic deployment by assigning a subscription number to the terminal (**as of R6.2 only)**
- Deployment from a dedicated Excel file

### 7.6.1 DEPLOYING MITEL 6000 SIP PHONES THROUGH MANUAL LOGIN

Refer to Chapter 6.8.1 for the principle and procedure to follow to deploy Mitel 6000 SIP Phones through manual login.

*The external DHCP server will also provide Mitel 6000 SIP Phone with the IP address of the external FTP server and the account (connexio/connexio) to which Mitel 6000 SIP Phone will connect to download its production software release and global deployment data configuration file.*

When the terminal is registered for the first time (first REGISTER), s*ome* logout/login operations are performed on the terminal, or when the terminal software release is updated*,* some SNMP traps are sent by the PBX to MiVoice 5000 Manager, and the TMA inventory is updated.

Once Mitel 6000 SIP Phones are known to the TMA inventory, day-to-day management of these terminals becomes possible with TMA (see Chapter 6.15).

**Note : This deployment method does not need the use of the TMA deployment function.**

## 7.6.2 DEPLOYING MITEL 6000 SIP PHONES VIA MIVOICE 5000 USER PORTAL

Refer to Chapter 6.8.2 for the principle and procedure to follow to deploy Mitel 6000 SIP Phones via the MiVoice 5000 User Portal.

*The external DHCP server will also provide Mitel 6000 SIP Phone with the IP address of the external FTP server and the account (connexio/connexio) to which Mitel 6000 SIP Phone will connect to download its production software release and global deployment data configuration file.*

When the terminal is registered for the first time (first REGISTER), s*ome* logout/login operations are performed on the terminal, or when the terminal software release is updated*,* some SNMP traps are sent by the PBX to MiVoice 5000 Manager, and the TMA inventory is updated.

Once Mitel 6000 SIP Phones are known to the TMA inventory, day-to-day management of these terminals becomes possible with TMA (see Chapter 6.15).

**Note : This deployment method does not need the use of the TMA deployment function.**

## 7.6.3 DEPLOYING MITEL 6000 SIP PHONES AUTOMATICALLY

Refer to Chapter 6.8.3 for the principle and procedure to follow to deploy Mitel 6000 SIP Phones automatically.

*The external DHCP server will also provide Mitel 6000 SIP Phone with the IP address of the external FTP server and the account (connexio/connexio) to which Mitel 6000 SIP Phone will connect to download its production software release and global deployment data configuration file.*

When the terminal is registered for the first time (first REGISTER), s*ome* logout/login operations are performed on the terminal, or when the terminal software release is updated*,* some SNMP traps are sent by the PBX to MiVoice 5000 Manager, and the TMA inventory is updated.

Once Mitel 6000 SIP Phones are known to the TMA inventory, day-to-day management of these terminals becomes possible with TMA (see Chapter 6.15).

**Note : This deployment method does not need the use of the TMA deployment function.**

## 7.6.4 DEPLOYING MITEL 6000 SIP PHONES THROUGH AN EXCEL FORM

### *7.6.4.1 Principle*

Refer to Chapter 6.8.4.1.

### *7.6.4.2 Procedure*

#### 7.6.4.2.1 Collecting global and specific data via the Excel form

Refer to Chapter 6.8.4.2.1.

#### 7.6.4.2.2 Saving the global and specific data in .csv format

Refer to Chapter 6.8.4.2.2.

#### 7.6.4.2.3 Configuring external FTP server(s)

**Note : Concerning the actual configuration of an external FTP server on Windows 2000/2003 server or MiVoice 5000, refer to Chapter 11.**

To create or add a new external FTP storage server and define its configuration parameters, proceed as follows.

- Click the menu 

.
- Select **Region** and the **Multisite** concerned.

**Note : TMA retrieves the configuration of the managed regions, multi-sites and sites from MiVoice 5000 Manager.**

- Click **Add new server**.
- Define the following parameters:
  - Name: the name field is obligatory and allows the FTP server to be identified.
  - IP address: enter the the IP address of the external FTP server. This field is mandatory.
  - Port: the default FTP server listening port is 21. Its value cannot be modified.

**Note : The Subnet mask and Subnet address fields can be configured by clicking the Advanced configuration button. These two parameters are optional. They must be entered only if two FTP servers are attached to the same site. They are used to define the subnet of terminals concerned by this FTP server.**

  - **List of sites attached to the server:** click **Modify list of sites** to define the sites attached to this FTP server. In the site list management window, select the site(s) by ticking them individually or clicking All to select all of them. Then click **Save** and close the window either by clicking the **Close window** link, or by clicking  on the top right side of the window.
  - **Write login / Write password:** account used by TMA in nominal mode to update the FTP server.
  - **Test write login / Test write password:** account used by TMA in test mode to update the FTP server.
  - **Terminal login / Terminal password:** account used by terminals in nominal mode.
  - **Test terminal login / Test terminal password:** account used by terminals in test mode.

**Note : These four logins/passwords must be defined for the 53xxip range and 6xxxi range.**

**Recovering the login/password defined by default on the integrated FTP server of Mitel 5000 Gateways or MiVoice 5000 Server**

The accounts defined by default for an integrated server, if appropriate, may be restored automatically by clicking **Initialize embedded**.

- Click **Confirm** to back up the current FTP server configuration:
  - the window then displays the FTP server(s) defined for the **Region** and **Multisite** concerned by showing the related site(s).
  - A link allows the current FTP server configuration to be displayed and/or modified.
  - A link allows the current FTP server configuration to be deleted.

#### 7.6.4.2.4 Installing the software package to be deployed

Refer to Section 6.15.4.

#### 7.6.4.2.5 Deploying the terminal software release and configuration files on the deployment FTP server

To deploy the terminal software release, language files and configuration files for the global and specific data of Mitel 6000 SIP Phones on the deployment FTP server, proceed as follows.

- Click the menu 

.
- Select **Region** and the **Multisite** concerned then the **6xxxi** series.

**Note : TMA retrieves the configuration of the managed regions, multi-sites and sites from MiVoice 5000 Manager.**

- In the **List of FTP servers** column, click the FTP server(s) on which the terminal software release and configuration files will be placed.

**Note : If only one FTP server is defined, this will be selected by default.**

- Select the **Software version** to be deployed.

**Note : If only one software release is installed, it will be selected by default.**

- Select the **Global (csv) file** to be deployed:
  - Click **Browse** then select the .csv file to import and which corresponds to the global data of Mitel 6000 SIP Phone from the collection. Click **Open.**
- Select the **Specific (csv) file** to be deployed:
  - Click **Browse** then select the .csv file to import and which corresponds to the specific data of Mitel 6000 SIP Phones from the collection. Click **Open.**
- Click **Validate** to start deploying the terminal software release and the configuration files of Mitel 6000 SIP Phones: a message indicates that the deployment has been implemented.
- The following files are then placed automatically by TMA in the storage directory of the deployment FTP server:
  - The terminal software releases <**such as poste>.st** (example: 55i.st)
  - The global data file **aastra.cfg**
  - The specific data files @MAC.cfg (example: 00085D3A2451.cfg)
  - The language pack files: **lang_<ISO 639>_<ISO 3166>.txt** or **lang_<ISO 639>.txt** (example: lang_fr_ca.txt or lang_de.txt)

**Note : The global and specific data is automatically changed to a format that is compatible with Mitel 6000 SIP Phones by TMA.**

- The terminals' global and specific data files are equally copied automatically to the tree on which are stored on the MiVoice 5000 Manager server PC, for the multi-site in question and Mitel 6000 SIP Phone, the configuration data used by TMA for these terminals. This prevents the global and specific data from being entered twice in TMA for day-to-day management of these terminals.

#### 7.6.4.2.6 Checking that the deployment process is working correctly

This operation is used to ensure that the deployment operation has been performed correctly.

- Click the menu. 

- Check in **Action monitoring,** the status of the deployment operation:
  - If the deployment operation was successful, the status indicates: **Success**
- Check in the **Event log,** the status of the deployment operation:
  - If the deployment operation was successful, the status indicates: **Action successful, Transfer of RA.B_67xxi_XX_YY data to FTP OK (n/n files).**
  - The number of transferred files is used to ensure that all the files have actually been placed in the deployment FTP server storage directory.

#### 7.6.4.2.7 Modifying the external DHCP server configuration before deployment

This modification is used to temporarily define, during this deployment phase, the account which Mitel 6000 SIP Phone must use to connect to the storage directory in which all the files have just been placed (the account to use is the account defined in write mode for Mitel 6000 SIP Phone in the TMA server configuration menu).

#### 7.6.4.2.8 Connecting the terminals to the local area network

- The operator connects the terminal to the local area network:
  - The terminal retrieves from the DHCP server the IP address of the deployment FTP server with the account to which it must connect.
  - The terminal connects to the deployment FTP server and updates its software release if necessary. The terminal also retrieves its global and specific data configuration files.
  - The terminal registers automatically to its reference site from the information contained in its global and specific data configuration files and is then visible in the TMA inventory.

#### 7.6.4.2.9 Modifying the external DHCP server configuration after deployment

After the deployment phase, this modification is used to reset the login/password **connexio:connexio** defined by default in the external DHCP server for deployment through deployment login or manual login of Mitel 6000 SIP Phones.

#### 7.6.4.2.10 Inventory of the configuration

TMA gives the configuration inventory of Mitel 6000 SIP Phones, after first deployment.

**Note : The inventory lists all the terminals on the installation.**

When the terminal is first registered, an SNMP trap is sent by the PBX to MiVoice 5000 Manager. This trap contains the data stored in MiVoice 5000 Manager and which is used by TMA to update the information displayed in the inventory concerning Mitel 6000 SIP Phones.

The main data contained in the trap for a Mitel 6000 SIP Phone are:

- The terminal directory number

- The terminal label
- The possibility to log out the terminal periodically
- The reference site
- The terminal range and model
- Terminal software release
- Terminal IP address
- Terminal MAC address
- The extension number (for a multi-line terminal)
- The index associated with the terminal's global data file
- The index associated with the terminal's specific data file

The other fields do not concern this environment.

To display the inventory of Mitel 6000 SIP Phone configuration in TMA, proceed as follows:

- Click the menu 

.
- Select the **67xxi range** and possibly the **model**.
- By default, the index associated with the terminal's global data file is "**1**".
- Information display depends on the filter used. This filter is activated by clicking the icon. 
- If possible, apply a filter to the current inventory based on:
  - The subscription reference site
  - The terminal subscription number
  - The terminal IP address
  - The terminal software release (production, test release, etc.)
  - The terminal global data index
  - The terminal specific data index
  - The terminal MAC address
  - Terminal encryption configuration:
    - SRTP (and TLS) mode activated
    - TLS mode activated
    - No encryption activated.



**Note : The joker * may be applied to the parameters Number, IP address and Mac address by placing them at the end of the parameter value.**

- Click**Filter** to apply the filter to the current inventory.

The **logged** column is used to indicate whether Mitel 6000 SIP Phone is registered on its reference site (green tick) or whether the terminal is not registered on its reference site (red cross).



**Note : If the terminal is not registered on its reference site, a tooltip indicates the possible reason why the registration failed or whether the terminal is a general-purpose one.**

As of R3.1C, the **Encryption** column indicates the encryption status of Mitel 6000 SIP Phones:

- Encrypted terminal in SRTP (and TLS): 

- Encrypted terminal in TLS 
- Terminal not encrypted: Empty
- Information not available: 

  (configuration file not present or encryption parameters not found)

### 7.6.5 DEFINING THE PRODUCTION TERMINAL SOFTWARE PACKAGE

This procedure is used to define the production terminal software package.

- Click the menu 

.
- Select **Region** and the **Multisite** concerned then the **6xxxi** series.
- In a configuration with several multi-sites, a new window opens: select the region, standalone multi-site/site then click **Continue**.



**Note : TMA retrieves the configuration of the managed regions, multi-sites and sites from MiVoice 5000 Manager.**

- Click **Change**.
- Click the link **Configure production software release**:
- Select the previously installed terminal software package then click **Validate**.

### 7.6.6 DEFINING THE PARAMETERS OF THE SOFTWARE PACKAGE USED WITH THE PRODUCTION RELEASE

For a given software release, this procedure is used to assign the parameters for each terminal range. The range of each parameter is given.



**Note : This distribution is necessary if you wish to update the terminal data.**

A parameter is defined either:

- In the Mitel 6000 SIP Phone global data configuration file (Range = Global)
- In the Mitel 6000 SIP Phone specific data configuration file (Range = Specific)
- In the DHCP server (Scope = DHCP)
- Or in none of the previous scopes; so this parameter is not managed (Scope = Ignored).

This distribution must be made for each software release installed.

- Click the **Terminals configuration** menu.
- Select the **Region** and **Multisite** concerned.
- Select the **6xxxi** range.
- In the field **Version to configure**, select the terminal software package concerned by the distribution.

A distribution of the parameters in form of tabs is only displayed for Mitel 6000 SIP Phones:

- **Encryption**: encryption parameters for Mitel 6000 SIP Phones
- **Config**: the usual configuration parameters

- **TimeZone**: date and time, NTP server, time zone configuration parameters
- **Network**: network parameters (DHCP, VLAN, LLDP,..)
- **RFC2833**: RFC2833 / SIP INFO configuration parameters
- **802.1X**: 802.1X configuration parameters
- **RTCP**: RTCP configuration parameters
- **Directory**: configuration parameters used to access the LDAP directory and Exchange contacts (function available as of R6.2)
- **Expert**: all the other parameters not available in the previous tabs.

**Note : To facilitate the introduction of certain features (encryption, etc.), some parameters are available twice in the tab:**

- **in the upper part, the parameters have a range and some fixed values.**
- **in the lower part, the same parameters have a default value which may differ and a range set to ignored.**

- Select a tab then define the range of each parameter available in this tab like in the Excel form during data collection.

**Note : Pop-ups are used to obtain the definition of each parameter. They appear when the cursor is placed over the name of the parameter.**

- Click **Save**:
  - Clicking **Distribute** displays a confirmation message before the distribution of parameters is locked for this software release.

**Note : It is possible from MiVoice 5000 Manager V2.3A to unlock the distribution if necessary. In this case, it is mandatory after the new parameter allocation to start some global and specific data update actions so as to take into account the parameter values whose assignment has changed.**

- The **Initialise** button restores the factory distribution of the parameters associated with this software release.

**Note : The parameters managed by DHCP, or ignored, are displayed for information purposes only.**

After the distribution operation, it is possible to perform, if necessary, an update of the global and specific data of Mitel 6000 SIP Phones. Refer to Sections 7.8.2 and 7.8.3 for more information about the procedure to follow.

# 7.7 DEPLOYING MIVOICE 5300 IP PHONES

Prerequisites:

- The DHCP and FTP servers are working.
- Subscriptions exist on each iPBX.

A global parameter can be configured to disable the free seating function. In this case (parameter unticked, the impact is as follows:

- On Mitel 5300 SIP Phones, the Ident key remains displayed, but manual login from the terminals is rejected for all the Mitel 5300 SIP Phones on the installation.

This parameter is accessible via Menu **Telephony service** > **Subscribers** > **Terminals and Applications** > **6xxxi parameters**, and is called **Manual login authorisation on any terminal type**. By default, this parameter is enabled (ticked). This parameter is accessible if login via MiVoice 5000 User Portal is open.

MiVoice 5300 IP Phones can be deployed in two ways:

- Deploy MiVoice 5300 IP Phones automatically via the **manual login** function,
- Deploy the terminals via an Excel form.

## 7.7.1 DEPLOYING MIVOICE 5300 IP PHONES AUTOMATICALLY VIA THE MANUAL LOGIN FUNCTION

Refer to Chapter 6.9.1 à la page 126 for the principle and procedure to follow to deploy MiVoice 5300 IP Phones through manual login.

When the terminal is registered for the first time (first REGISTER), s*ome* logout/login operations are performed on the terminal, or when the terminal software release is updated, some SNMP traps are sent by the PBX to MiVoice 5000 Manager, and the TMA inventory is updated.

Once MiVoice 5300 IP Phones are known to the TMA inventory, day-to-day management of these terminals becomes possible with TMA (see Chapter ).



**Note : This deployment method does not need the use of the TMA deployment function.**

## 7.7.2 DEPLOYING MIVOICE 5300 IP PHONES THROUGH AN EXCEL FORM

### *7.7.2.1 Principle*

Refer to Chapter 6.8.4.1 à la page 120.

### *7.7.2.2 Procedure*

#### 7.7.2.2.1 Collecting global and specific data via the Excel form

Refer to Chapter 6.8.4.2.1 à la page 121.

#### 7.7.2.2.2 Saving the global and specific data in .csv format

Refer to Chapter 6.8.4.2.2 à la page 121.

#### 7.7.2.2.3 Configuring external FTP server(s)

Refer to Chapter 7.6.4.2.3 à la page 202.

#### 7.7.2.2.4 Installing the software package to be deployed

See Chapter 7.6.4.2.4 à la page 203 for information on how to install a MiVoice 5300 IP Phone software package.

#### 7.7.2.2.5 Deploying the terminal software release and configuration files on the deployment FTP server

See Chapter 7.6.4.2.5 à la page 203 for information on how to deploy the terminal software release and configuration files to the deployment FTP server by selecting the **53xxip** range.

#### 7.7.2.2.6 Checking that the deployment process is working correctly

This operation is used to ensure that the deployment operation has been performed correctly.

- Click the menu. 

- Check in **Action monitoring,** the status of the deployment operation:
  - If the deployment operation was successful, the status indicates: **Success**
- Check in the **Event log,** the status of the deployment operation:
  - If the deployment operation was successful, the status indicates: **Action successful, Transfer of RA.B_53xxip_XX_YY data to FTP OK (n/n files).**
  - The number of transferred files is used to ensure that all the files have actually been placed in the deployment FTP server storage directory.

#### 7.7.2.2.7 Connecting the terminals to the local area network

- The operator connects the terminal to the local area network by first entering its directory number if the specific data is indexed by the directory number:
  - The terminal retrieves the IP address of the deployment FTP server from the DHCP server.
  - The terminal connects to the deployment FTP server and updates its software release if necessary. The terminal also retrieves its global and specific data configuration files.
  - The terminal registers automatically to its reference site from the information contained in its global and specific data configuration files and is then visible in the TMA inventory.

#### 7.7.2.2.8 Inventory of the configuration

TMA gives the configuration inventory of MiVoice 5300 IP Phones, after first deployment.

**Note : The inventory lists all the terminals on the installation.**

When the terminal is first registered, an SNMP trap is sent by the PBX to MiVoice 5000 Manager. This trap contains the data stored in MiVoice 5000 Manager and which is used by TMA to update the information displayed in the inventory concerning MiVoice 5300 IP Phones.

The main data contained in the trap for a MiVoice 5300 IP Phone are:

- The terminal directory number
- The reference site
- The terminal range
- The terminal model
- Terminal software release
- Terminal IP address
- Terminal MAC address

- The index associated with the terminal's global data file
- The index associated with the terminal's specific data file
- The index of the terminal's TM (Terminal Model) (visible in the export file only)

**Note : By default, the value of the global and specific data index of a MiVoice 5300 IP Phone is 00. During a deployment, these indices are not managed and their value remain 00.**

To display the inventory of MiVoice 5300 IP Phone configuration in TMA, proceed as follows:

- Click the menu Inventory .
- Select the **Region** and **Multisite** concerned then the **53xxip** series and possibly the **Model**.
- The terminals are not associated with a production software release or a test software release because at the moment the release used to deploy the terminals has not been configured in TMA.
- Information display depends on the filter used. This filter is activated by clicking the icon.
- If possible, apply a filter to the current inventory based on:
  - The subscription reference site
  - The terminal subscription number
  - The terminal IP address
  - The terminal software release (production, test release, etc.)
  - The terminal global data index
  - The terminal specific data index
  - The terminal MAC address
  - Terminal encryption configuration:
    - SRTP (and TLS) mode activated
    - No encryption activated

The **logged** column is used to indicate whether MiVoice 5300 IP Phone is registered on its reference site (green tick) or whether the terminal is not registered on its reference site (red cross).

If the terminal is not registered on its reference site, a tooltip indicates the possible reason why the registration failed or whether the terminal is a general-purpose one.

As of R3.1C, the **Encryption** column indicates the encryption status of MiVoice 5300 IP Phones:

- Encrypted terminal in SRTP (and TLS):
- Terminal not encrypted: Empty
- Information not available:

  (configuration file not present or encryption parameters not found)

#### 7.7.2.3 *Defining the production version*

This procedure is used to define the production software release.

In the present case, following the deployment of terminal release, this latter will be defined as the production release.

- Click the Software managment menu.
- Select **Region** and the **Multisite** concerned then the **53xxip** series.

**Note : TMA retrieves the configuration of the managed regions, multi-sites and sites from MiVoice 5000 Manager.**

- Click **Change**.
- Click the link **Configure production software release**:
  - select the version and click **confirm**.

Terminal release is now the production release and appears in green in the inventory.

#### 7.7.2.4 *Distributing the production version parameters*

This procedure is used to distribute the parameters associated with a software release installed in TMA. . The range of each parameter is given.

**Note : This distribution is necessary if you wish to update the terminal data.**

A parameter is defined either:

- In the MiVoice 5300 IP Phone global data configuration file
- In the MiVoice 5300 IP Phone specific data configuration file
- In the DHCP server
- Or in none of the previous ranges, so this parameter is not managed.

This distribution must be made for each software release installed and configured in TMA as production release or test release.

- Click theTerminals configuration menu.
- Select **Region** and the **Multisite** concerned then the **53xxip** series.

**Note : TMA retrieves the configuration of the managed regions, multi-sites and sites from MiVoice 5000 Manager.**

- In the field **Version to configure**, select the version concerned by the distribution.
- Define the range of each parameter like in the Excel form during data collection.

**Note : Pop-ups are used to obtain the definition of each parameter. They appear when the cursor is placed over the name of the parameter.**

**Note : Tab-based parameter distribution is not available for MiVoice 5300 IP Phones.**

- Click **Save**:
  - Clicking **Distribute** displays a confirmation message before the distribution of parameters is locked for this software release.



**Note : It is possible from MiVoice 5000 Manager V2.3A to unlock the distribution if necessary. In this case, it is mandatory after the new parameter allocation to start some global and specific data update actions so as to take into account the parameter values whose assignment has changed.**

  - The **Initialise** button restores the factory distribution of the parameters associated with this software release.



**Note : The parameters managed by DHCP, or ignored, are displayed for information purposes only.**

After the distribution operation, it is possible to perform, if necessary, an update of the global and specific data of MiVoice 5300 IP Phones.

Refer to Chapter 7.10.2 and 7.10.3 for more information about the procedure to follow.

# 7.8 UPDATING MITEL 6000 SIP PHONES MANUALLY

This chapter describes how to manually update Mitel 6000 SIP Phones.

Once a Mitel 6000 SIP Phone is known in the TMA inventory, this terminal is managed by TMA, and it can be updated on a daily basis.

**Note : Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.**

**Note : Mitel 6000 SIP Phone software and global data can be updated without any Mitel 6000 SIP Phone being physically connected to the network.**

## 7.8.1 PRINCIPLE

Mitel 6000 SIP Phones are updated manually from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.14.1 on Page 139).

**Note : When the terminal is registered for the first time (first REGISTER), some logout/login operations are performed on the terminal, or when the terminal software release is updated, some SNMP traps are sent by the PBX to MiVoice 5000 Manager, and the inventory of the TMA integrated into MiVoice 5000 Manager is updated.**

## 7.8.2 GLOBAL DATA UPDATE

This procedure applies once a terminal appears in the TMA application inventory. This procedure updates the global data of all the Mitel 6000 SIP Phones.

**Note : lLogged and unlogged terminals are visible in the TMA inventory and are managed by TMA.**

The global data of Mitel 6000 SIP Phones are updated from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.15.2 à la page 143).

## 7.8.3 SPECIFIC DATA UPDATE

This procedure applies once a terminal appears in the TMA application inventory. This procedure updates the common specific data of a list of Mitel 6000 SIP Phones.

*Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.*

The specific data of Mitel 6000 SIP Phones are updated from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.15.3 à la page 146).

### 7.8.4 UPDATING MITEL 6000 SIP PHONE SOFTWARE RELEASE

This procedure applies once a terminal appears in the TMA application inventory. This procedure is used to update the software release of all Mitel 6000 SIP Phones known to the inventory.

*Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.*

The software release of Mitel 6000 SIP Phones are updated from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Section 6.15.4).

The only differences are:

**1 - For the list of components to download in the Software Management menu:**

Once the version selected, when the list of components of the package is presented, it is given for information (shaded boxes).

No change is possible because all the components are to download.

**2- For the update in versions lower than R6.5:**

The old method of downloading packages "posts" is still available but the function has been renamed to "A**dd versions (packages less than R6.5)"**.

### 7.8.5 DISTRIBUTING THE PARAMETERS OF THE NEW PRODUCTION RELEASE

This procedure is used to distribute the parameters associated with a new software release installed in TMA. The range of each parameter is given.

A parameter is defined either:

- In the Mitel 6000 SIP Phone global data configuration file
- In the Mitel 6000 SIP Phone specific data configuration file
- In the DHCP server
- Or in none of the previous ranges, so this parameter is not managed.

The procedure for distributing the parameters of the new production release of Mitel 6000 SIP Phones from the integrated TMA in MiVoice 5000 Manager is the same as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.15.5 à la page 153).

## 7.8.6 MANAGING THE LIST OF TERMINALS FOR MITEL 6000 SIP PHONES

This procedure is used to define a list of terminals for all models of Mitel 6000 SIP Phones.

This list is used either:

- In nominal mode, to update some specific data on a global or restricted range, or
- In test mode, to update the terminals' software release, global data and specific data on a limited range.



**ATTENTION : In test mode, the list contains a maximum of 10 terminals.**



**ATTENTION : A terminal may be assigned only to one list at a time.**

The list used in test mode to update the terminal software release must be the same as the one used to update the global data and specific data.

### *7.8.6.1 Defining a new list by entering the terminals one by one*

A new list is defined from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.15.6.1 à la page 155).

### *7.8.6.2 Defining a new list from a site*

- Click the **Inventory** menu.
- Select the **Region** and **Multisite** concerned.
- Select the **67xxi range** and possibly the **model**.
- Click **List management:**
  - The **terminal range**: **6xxxi**
  - The Telephone set **model** concerned
- Click **Create a list from a site**.

A new window opens. This allows you to define a list of terminals from the terminals known to the inventory for this site and for the series of terminals concerned.

- Select any of the sites presented in the window by clicking it.
- In the right area, enter the **List name** then click **Confirm**.
  - The message has been successfully saved.
- Close the window either by clicking the **Close window** link, or by clicking on the top right side of the window.
- The list management window is refreshed and then displays:
  - The list name
  - The number of terminals contained on the list
  - The **Action** field used to delete or modify the displayed list.
- Click **Return** to return to the **Inventory** window.

### *7.8.6.3 Modifying a list*

A list is modified from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.15.6.2 à la page 155).

#### *7.8.6.4 Deleting a list*

A list is deleted from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.15.6.3 à la page 156).

# 7.9 TEST MODE FOR MITEL 6000 SIP PHONES

The test mode is used to update the terminals' software release, global data and specific data on a range limited to 10 terminals maximum. This function is used to test a new terminal software application or new function/configuration on a small number of terminals before exposing it to all the terminals.

The list of terminals used in test mode to update the terminal software release must be the same as the one used to update the global data and specific data of the tested terminals.

The different files (terminal software, global or specific data) are stored in the **test directory** defined in the external FTP server configuration.

## 7.9.1 UPDATING MITEL 6000 SIP PHONE SOFTWARE RELEASE IN TEST MODE

This procedure applies once a terminal is registered to its reference site through any of the deployment methods described in the previous chapters. This procedure is used to update the software release of the Mitel 6000 SIP Phones known to the inventory and defined on a list containing at most 10 terminals.

The software release of Mitel 6000 SIP Phones is updated in test mode from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.16.1 à la page 156).

## 7.9.2 DISTRIBUTING THE NEW TEST SOFTWARE RELEASE PARAMETERS

The procedure for distributing the parameters of the new test release of Mitel 6000 SIP Phones from the integrated TMA in MiVoice 5000 Manager is the same as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.16.2 à la page 158).

**Note : In the field Version to configure, select the test version concerned by the distribution.**

## 7.9.3 UPDATING THE GLOBAL DATA OF THE TERMINALS USED WITH THE TEST SOFTWARE

This procedure is used to update the global data of Mitel 6000 SIP Phone in the test software release.

The global data of Mitel 6000 SIP Phones in test software release is updated from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.16.3 à la page 158).

**Note : In the field Version to configure, select the test version concerned by the distribution.**

## 7.9.4 UPDATING THE SPECIFIC DATA OF TERMINALS USED WITH THE TEST SOFTWARE

This procedure is used to update the specific data of Mitel 6000 SIP Phone in the test software release.

### *7.9.4.1 Updating the common specific data of terminals in the test software release*

This procedure is used to update the specific data of terminals in the test software release.

The common specific data of Mitel 6000 SIP Phones in test software release is updated from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.16.4.1 à la page 160).

**Note : In the field Version to configure select the test release.**

#### 7.9.4.2 *Updating the specific data of individual terminals used with the test software*

This procedure is used to update the special specific data of terminals in the test software release.

The special specific data of Mitel 6000 SIP Phones in test software release is updated from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.16.4.2 à la page 161).



**Note : In the field Version to configure select the test release.**

## 7.9.5 EXITING THE TEST MODE

This procedure is used to leave the test mode at the end of the test phase.

Two possibilities are available:

- The tested new software release is satisfactory: in this case, all the terminals on the installation must be updated with the new test software.
- The tested new software release is not satisfactory: in this case, only the tested terminals must be updated with the current production software.

### *7.9.5.1 Switching from test mode to production mode*

In this case, the test software release must be defined as the new production software release, and an update operation for this new production software release started on all the terminals.

The procedure for changing from test mode to production mode from the TMA integrated into MiVoice 5000 Manager is the same as the one described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.16.5.1 à la page 162).

### *7.9.5.2 Returning to the current version*

In this case, the test software release is not satisfactory. The terminals on the test list must be down-graded with the current production release. An update for this production software release must be started on all the terminals.

The procedure for returning to the current release from the TMA integrated into MiVoice 5000 Manager is the same as the one described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.16.5.2 à la page 163).

# 7.10 UPDATING MIVOICE 5300 IP PHONES MANUALLY

This chapter describes how to manually update MiVoice 5300 IP Phones.

Once a MiVoice 5300 IP Phone is known in the TMA inventory, this terminal is managed by TMA, and it can be updated on a daily basis.

**Note : Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.**

**Note : Mitel 6000 SIP Phone software and global data can be updated without any Mitel 6000 SIP Phone being physically connected to the network.**

## 7.10.1 PRINCIPLE

MiVoice 5300 IP Phones are updated manually from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.17 à la page 164).

**Note : When the terminal is registered for the first time (first REGISTER), some logout/login operations are performed on the terminal, or when the terminal software release is updated, some SNMP traps are sent by the PBX to MiVoice 5000 Manager, and the inventory of the TMA integrated into MiVoice 5000 Manager is updated.**

## 7.10.2 GLOBAL DATA UPDATE

This procedure applies once a terminal appears in the TMA application inventory. This procedure updates the global data of all the MiVoice 5300 IP Phones.

**Note : Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.**

The global data of MiVoice 5300 IP Phones are updated from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.15.2 à la page 143).

## 7.10.3 SPECIFIC DATA UPDATE

This procedure applies once a terminal appears in the TMA application inventory. This procedure updates the common specific data of a list of MiVoice 5300 IP Phones.

**Note : Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.**

The specific data of MiVoice 5300 IP Phones are updated from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter ).

## 7.10.4 UPDATING MIVOICE 5300 IP PHONE SOFTWARE RELEASE

This procedure applies once a terminal appears in the TMA application inventory. This procedure is used to update the software release of all MiVoice 5300 IP Phones known to the inventory.

**Note : Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.**

The software release of MiVoice 5300 IP Phones are updated from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.17.4 à la page 168).

### 7.10.5 DISTRIBUTING THE PARAMETERS OF THE NEW PRODUCTION RELEASE

This procedure is used to distribute the parameters associated with a new software release installed in TMA. The range of each parameter is given.

A parameter is defined either:

- In the MiVoice 5300 IP Phone global data configuration file
- In the MiVoice 5300 IP Phone specific data configuration file
- In the DHCP server
- Or in none of the previous ranges, so this parameter is not managed.

This distribution must be made for each software release installed and configured in TMA as production release or test release.

The procedure for distributing the parameters of the new production release of MiVoice 5300 IP Phones from the integrated TMA in MiVoice 5000 Manager is the same as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.15.5 à la page 153).

## 7.10.6 MANAGING THE LIST OF TERMINALS FOR MIVOICE 5300 IP PHONES

This procedure is used to define a list of terminals for all models of MiVoice 5300 IP Phones.
This list is used either:

- In nominal mode, to update some specific data on a global or restricted range, or
- In test mode, to update the terminals' software release, global data and specific data on a limited range.

**ATTENTION : In test mode, the list contains a maximum of 10 terminals.**

**ATTENTION : A terminal may be assigned only to one list at a time.**

The list used in test mode to update the terminal software release must be the same as the one used to update the global data and specific data.

### *7.10.6.1 Defining a new list by entering the terminals one by one*

A new list is defined from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.15.6.1 à la page 155).

### *7.10.6.2 Defining a new list from a site*

- Click the **Inventory** menu.
- Select the **Region** and **Multisite** concerned then the **53xxip** series and possibly the **Model**.
- Click **List management:**

A new window opens. This window gives the criteria concerned by the list creation:

  - The **Region** concerned
  - The **Multisite** concerned
  - The **terminal range**: **53xxip**
  - The Telephone set **model** concerned

- Click **Create a list from a site**.

A new window opens. This allows you to define a list of terminals from the terminals known to the inventory for this site and for the series of terminals concerned.

- Select any of the sites presented in the window by clicking it.
- In the right area, enter the **List name** then click **Confirm**.
  - The message has been successfully saved.
- Close the window either by clicking the **Close window** link, or by clicking on the top right side of the window.

- The list management window is refreshed and then displays:
  - The list name
  - The number of terminals contained on the list
  - The **Action** field used to delete or modify the displayed list.
- Click **Return** to return to the **Inventory** window.

#### *7.10.6.3 Modifying a list*

A list is modified from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.15.6.2 à la page 155).

#### *7.10.6.4 Deleting a list*

A list is deleted from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.15.6.3 à la page 156).

## 7.11 TEST MODE FOR MIVOICE 5300 IP PHONES

The test mode is used to update the terminals' software release, global data and specific data on a range limited to 10 terminals maximum. This function is used to test a new terminal software application or new function/configuration on a small number of terminals before exposing it to all the terminals.

The list of terminals used in test mode to update the terminal software release must be the same as the one used to update the global data and specific data of the tested terminals.

The different files (terminal software, global or specific data) are stored in the **test directory** defined in the FTP server configuration.

### 7.11.1 UPDATING MIVOICE 5300 IP PHONE SOFTWARE RELEASE IN TEST MODE

This procedure applies once a terminal is registered to its reference site through any of the deployment methods described in the previous chapters. This procedure is used to update the software release of the MiVoice 5300 IP Phones known to the inventory and defined on a list containing at most 10 terminals.

The software release of MiVoice 5300 IP Phones is updated in test mode from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.18.1 à la page 171).

### 7.11.2 DISTRIBUTING THE NEW TEST SOFTWARE RELEASE PARAMETERS

The procedure for distributing the parameters of the new test release of MiVoice 5300 IP Phones from the integrated TMA in MiVoice 5000 Manager is the same as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.16.2 à la page 158).



**Note : In the field Version to configure, select the test version concerned by the distribution.**

### 7.11.3 MIVOICE 5300 IP PHONE GLOBAL DATA UPDATE IN THE TEST SOFTWARE RELEASE

This procedure is used to update the global data of MiVoice 5300 IP Phone in the test software release.

The global data of MiVoice 5300 IP Phones in test software release is updated from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.16.3 à la page 158).



**Note : In the field Version to configure, select the test version concerned by the distribution.**

## 7.11.4 UPDATING THE SPECIFIC DATA OF MIVOICE 5300 IP PHONES IN THE TEST SOFTWARE RELEASE

This procedure is used to update the specific data of MiVoice 5300 IP Phone in the test software release.

### *7.11.4.1 Updating the common specific data of MiVoice 5300 IP Phones used with the test software*

This procedure is used to update the common specific data of MiVoice 5300 IP Phones in the test software release.

The common specific data of MiVoice 5300 IP Phones in test software release is updated from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.16.4.1 à la page 160).



**Note : In the field Version to configure select the test release.**

### *7.11.4.2 Updating the special specific data of MiVoice 5300 IP Phones used with the test software*

This procedure is used to update the special specific data of MiVoice 5300 IP Phones in the test software release.

The special specific data of Mitel 6000 SIP Phones in test software release is updated from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.16.4.2 à la page 161).



**Note : In the field Version to configure select the test release.**

## 7.11.5 EXITING THE TEST MODE

This procedure is used to leave the test mode at the end of the test phase.

Two possibilities are available:

- The tested new software release is satisfactory: in this case, all the terminals on the installation must be updated with the new test software.
- The tested new software release is not satisfactory: in this case, only the tested terminals must be updated with the current production software.

### *7.11.5.1 Switching from test mode to production mode*

In this case, the test software release must be defined as the new production software release, and an update operation for this new production software release started on all the terminals.

The procedure for changing from test mode to production mode from the TMA integrated into MiVoice 5000 Manager is the same as the one described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.16.5.1 à la page 162).

### *7.11.5.2 Returning to the current version*

In this case, the test software release is not satisfactory. The terminals on the test list must be downgraded with the current production release. An update for this production software release must be started on all the terminals.

The procedure for returning to the current release from the TMA integrated into MiVoice 5000 Manager is the same as the one described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.16.5.2 à la page 163).

# 7.12 MANAGING MIVOICE 5300 DIGITAL PHONES (TDM)

For TDM MiVoice 5300 Digital Phone, TMA offers the following functions:

- Inventory
- Updating terminal software (production release and test release)
- Actions display.

## 7.12.1 INVENTORY OF MIVOICE 5300 DIGITAL PHONES

TMA gives the configuration inventory of MiVoice 5300 Digital Phones, after first deployment.

The main data contained in the trap for a MiVoice 5300 Digital Phone are:

- **The subscription reference site**
- The terminal subscription number
- The terminal range and model
- The Terminal software release
- The terminal group site number (local or remote site)
- The number of the cluster on which the subscription is declared and the terminal connected
- The physical location on which the subscription is declared, and the terminal connected (cabinet, card, trunk).

The other fields do not concern this environment.

**Note : If a MiVoice 5300 Digital Phone is inaccessible (card out of service) or is parked, the inventory associated with this terminal is refreshed. The previous physical location, as well as its type and model, is stored.**

To display the inventory of MiVoice 5300 Digital Phone configuration in TMA, proceed as follows:

- Click the **Inventory** menu.
- Select the **Region** and **Multisite**.
- Select the **53xx** range and possibly the **Model**.

Information display depends on the filter used. This filter is activated by clicking the icon.

- If possible, apply a filter to the current inventory based on:
  - The subscription community
  - The subscription reference site
  - The terminal subscription number
  - The terminal software release (production, test release, etc.)

**Note : The joker * may be applied to the Number parameters by placing it at the end of the parameter value.**

- Click**Filter** to apply the filter to the current inventory.

The version of the terminals in the **Software release** column is green in colour if it is the same as the terminal software release defined as the production software release.

The **List management** window is used to define the list of terminals to which the test version update will apply.

## 7.12.2 MANAGING THE LIST OF TERMINALS FOR MIVOICE 5300 DIGITAL PHONES

This procedure is used to define a list of terminals for all models of MiVoice 5300 Digital Phones. This list is used in test mode to upgrade the software release of terminals over a limited range.



**ATTENTION : In test mode, the list contains a maximum of 10 terminals.**



**ATTENTION : A terminal may be assigned only to one list at a time.**

### *7.12.2.1 Defining a new list by entering the terminals one by one*

A new list is defined from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.15.6.1).

### *7.12.2.2 Defining a new list from a site*

- Click the **Inventory** menu.
- Select the **Region** and **Multisite**.
- Select the **53xx** range and possibly the **Model**.
- Click **List management:**

  A new window opens. This window gives the criteria concerned by the list creation:

  - The **Region** concerned
  - The **Multisite** concerned
  - The **terminal range**: **53xx**
  - The Telephone set **model** concerned
- Click **Create a list from a site**.

  A new window opens. This allows you to define a list of terminals from the terminals known to the inventory for this site and for the series of terminals concerned.
- Select any of the sites presented in the window by clicking it.
- In the right area, enter the **List name** then click **Confirm**.
  - The message has been successfully saved.
- Close the window either by clicking the **Close window** link, or by clicking on the top right side of the window.
- The list management window is refreshed and then displays:
  - The list name
  - The number of terminals contained on the list
  - The **Action** field used to delete or modify the displayed list.
- Click **Return** to return to the **Inventory** window.

### *7.12.2.3 Modifying a list*

A list is modified from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.15.6.2 à la page 155).

#### 7.12.2.4 *Deleting a list*

A list is deleted from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Chapter 6.15.6.3 à la page 156).

### 7.12.3 UPDATING THE SOFTWARE RELEASE OF MIVOICE 5300 DIGITAL PHONES

This procedure is used to update the software release of all MiVoice 5300 Digital Phones known to the inventory.

**Note : During each MiVoice 5300 Digital Phone update operation (software), TMA checks the accessibility of the sites concerned by the action. In case of error during this check, the action is not performed.**

#### 7.12.3.1 *Installing the new software release to be deployed*

To install the new software release to be updated, use the MiVoice 5000 software CD-ROM containing the new software release then proceed as follows:

- Place the MiVoice 5000 software DVD or CD-ROM in the Web Admin client PC DVD/CD-ROM drive.
- Click the **Sofware managment** menu.
- Select the **53xx** range.
- Click **Change**.
- Click the **Add versions** link:
  - a new window opens, showing the list of installed software releases. By default, this list is empty.
- Click **Browse**:
  - Go to the **sip_sets_tma** directory of the MiVoice 5000 software CD-ROM.
  - Select the corresponding tar.gz file for the terminal to be installed (example **R6.1_53xx_xx-_yy.tar.gz**) . Click **Open.**
  - Click Send: the terminal version is installed and then appears on the list of installed software releases. Close the window by clicking on the top right side of the window.

### 7.12.3.2 *Defining the new production release*

This procedure is used to define the new production software release.

Refer to the previous figure then

- Click the menu 

.
- Select the **53xx** range.
- Click **Change**.
- Click the link **Configure production software release**:
  - Select the new version and click **Validate**.

**Note : The new software release is now the production release and all the terminals appear in red in the inventory (terminals seen in another software release).**

### 7.12.3.3 *Starting the update of the new production release*

- Click **Return**.
- A new window opens.

This indicates the criteria concerned by the update of the new software release:

  - The **terminal range**: **53xx**
  - The **Deployment software release**concerned
- Enter the **Action name**.
- Select the **Software release** concerned.
- Select the **Type of update**:
  - Immediate
  - Deferred: specifies the date in DD/MM/YYYY format and time in HHMM format.

**Note : Clicking the icon opens the calendar so the date can be selected directly.**

- Click **Validate** to start updating the software release of all MiVoice 5300 Digital Phones.

**ATTENTION : The update concerns group n of MiVoice 5300 Digital Phones. Each group contains at most 20 terminals. It takes approximately 20 minutes to update a group. There are as many groups as required.**

### 7.12.4 CHECKING THAT THE UPDATE PROCESS IS WORKING CORRECTLY FOR THE PRODUCTION SOFTWARE RELEASE

This operation is used to ensure that the new software release has been correctly updated.

- Click the **Display actions** menu.
- Check in **Action monitoring,** the status of the production release update operation:
  - If the operation was successful, the status indicates: **Success**
- Click the  icon to view the progress of the on-going production release update operation.
  - A colour code is used to check whether the terminals have the expected software release (green colour) or not (red colour). This colour code is only significant for the last action of this type. The information displayed may or may not be filtered with this criterion.
- Check in the **Event log** the status of the terminal software release update operation.
  - If the operation was successful, the status indicates: **Action successful**

The system concerned by the action is also indicated.

# 7.13 TEST MODE FOR MIVOICE 5300 DIGITAL PHONES

The test mode is used to update the terminals' software release, global data and specific data on a range limited to 10 terminals maximum. This function is used to test a new terminal software application or new function/configuration on a small number of terminals before exposing it to all the terminals.

The list of terminals used in test mode to update the terminal software release must be the same as the one used to update the global data and specific data of the tested terminals.

## 7.13.1 UPDATING MIVOICE 5300 DIGITAL PHONE SOFTWARE RELEASE IN TEST MODE

This procedure applies once a terminal appears in the TMA application inventory. This procedure is used to update the software release of the MiVoice 5300 Digital Phones known to the inventory and defined on a list containing at most 10 terminals.

In the example below:

- The production release = **R6.1_53xx_A2_00**
- The test release = **R6.1_53xx_A3_00.**

**ATTENTION : In test mode, only one software release update operation can be performed at a time for a list of terminals.**

### *7.13.1.1 Defining a test list*

See Section 7.12.2 à la page 228 for how to define a list of terminals containing a maximum of 10 terminals.

This list, called **test** , will be used in the procedure described below.

**ATTENTION : A list used by an on-going test cannot be deleted or modified.**

### *7.13.1.2 Installing the new test software release*

Refer to Section 6.15.4.

## 7.13.2 DEFINING THE NEW TEST VERSION

This procedure is used to define the new test software release.

- Click the **Sotware managment** menu.
- Select the **53xx** range.
- Click **Change**.
- Click the link **Configure test software release**:
  - Select the new release **R6.1_53xx_A3_00** and click **Validate**.

**Note : The new software release R6.1_53xx_A3_00 is now the test release.**

## 7.13.3 STARTING THE UPDATE OF THE NEW TEST VERSION

- Click **Return**.
- A new window opens.

  This indicates the criteria concerned by the update of the new software release:

- The **terminal range**: **53xx**
- The **Deployment software release**concerned: **R6.1_53xx_A2_00**
- The **Test software release**concerned: **R6.1_53xx_A3_00**

- Enter the **Action name**.
- Select the test **Software release** concerned: **R6.1_53xx_A3_00**
- Select the list to use in test mode: **test**
  - The **List details** link is used to display the terminals contained on the selected list.
- Select the **Type of update**:
  - Immediate
  - Deferred: specifies the date in DD/MM/YYYY format and time in HHMM format.



**Note :** **Clicking the icon opens the calendar so the date can be selected directly.**

- Click **Validate** to start updating the software release of all MiVoice 5300 Digital Phones.

### 7.13.4 CHECKING THAT THE UPDATE PROCESS IS WORKING CORRECTLY FOR THE TEST SOFTWARE RELEASE

This operation is used to ensure that the new test software release has been correctly updated.

- Click the menu Display actions.
- Check in **Action monitoring,** the status of the test version update operation: if the operation is successful, the status displays: **Success**
- Click the icon to view the progress of the on-going test software release update operation.
  - A colour code is used to check whether the terminals have the expected software release (green colour) or not (red colour). This colour code is only significant for the last action of this type. The information displayed may or may not be filtered with this criterion.
  - The **List** field displays the list used in test mode: **test**
  - The **Test** field is used to check whether or not the on-going operation is in test mode.
- Check in the **Event log** the status of the test software release update operation.
  - If the operation was successful, the status indicates: **Action successful**
  - The number of transferred files is used to check that all new test software release files have actually been placed in the test storage directory of the FTP server used for day-to-day terminal management in test mode.

### 7.13.5 EXITING THE TEST MODE

This procedure is used to leave the test mode at the end of the test phase.

Two possibilities are available:

- The tested new software release is satisfactory: in this case, all the terminals on the installation must be updated with the new test software.
- The tested new software release is not satisfactory: in this case, only the tested terminals must be updated with the current production software.

#### *7.13.5.1 Switching from test mode to production mode*

In this case, the test software release must be defined as the new production software release, and an update operation for this new production software release started on all the terminals.

In the example below the initial situation is as follows:

- Production release = **R6.1_53xx_A2_00**
- Test release = **R6.1_53xx_A3_00**

- Click the **Software managment** menu.
- Select the **53xx** range.
- Click **Change**.
- Click the link **Configure deployment software version**:
  - Select release **R6.1_53xx_A3_00** and click **Validate**.

  The situation is now:
  - Deployment release = **R6.1_53xx_A3_00**
  - No test version defined.
- Click **Return**.
- A new window opens.

This indicates the criteria concerned by the update of the new software release:

- The **terminal range**: **53xx**
- The **Deployment software release**concerned: **R6.1_53xx_A3_00**

- Enter the **Action name**.
- Select the **Software release** concerned: **R6.1_53xx_A3_00**
- Select the **Type of update**:
  - Immediate
  - Deferred: specifies the date in DD/MM/YYYY format and time in HHMM format.

**Note : Clicking the icon opens the calendar so the date can be selected directly.**

- Click **Validate** to start updating the production software release of all MiVoice 5300 Digital Phones.

#### *7.13.5.2 Returning to the current version*

In this case, the test software release is not satisfactory. The terminals on the test list must be down-graded with the current production release. An update for this production software release must be started on all the terminals.

In the example below the initial situation is as follows:

- Production release = **R6.1_53xx_A2_00**
- Test release = **R6.1_53xx_A3_00**

- Click the **Software managment** menu.
- Select the **53xx** range.
- Enter the **Action name**.
- Select the **Software release** concerned: **R6.1_53xx_A2_00**
- Select the **Type of update**:
  - Immediate
  - Deferred: specifies the date in DD/MM/YYYY format and time in HHMM format.

**Note : Clicking the icon opens the calendar so the date can be selected directly.**

- Click **Validate** to start updating the current production software release of all MiVoice 5300 Digital Phones.

**Note : Only the terminals with the test software release will be updated with the current production software release because all the other terminals are already in the right version.**

# 7.14 MANAGING VIRTUAL TDM MIVOICE 5300 DIGITAL PHONES

In a multi-site configuration, this function is used to assign a terminal MiVoice 5300 Digital Phone physically connected to a Mitel 5000 Gateways system to a subscription declared on a remote site (generally MiVoice 5000 Server).

## 7.14.1 INVENTORY OF MIVOICE 5300 DIGITAL PHONES

Refer to Chapter 7.12.1 for more information about the procedure.

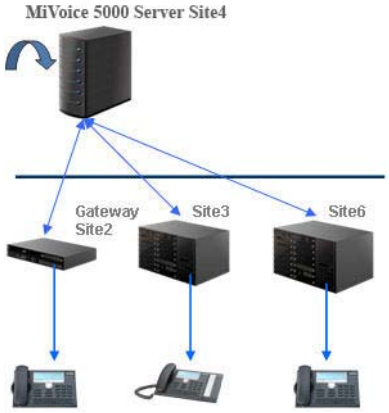
The **Site** column contains the name of the reference site on which the terminal MiVoice 5300 Digital Phone subscription is declared.

The **Site No.** column contains the number of the site to which the MiVoice 5300 Digital Phone subscription is physically connected.

## 7.14.2 UPDATING THE SOFTWARE RELEASE OF MIVOICE 5300 DIGITAL PHONES

Refer to Chapter 7.12.3 for more information about the procedure.

If all the MiVoice 5300 Digital Phone subscriptions are declared on MiVoice 5000 Server, the update operation will be handled by MiVoice 5000 Server:




- Copying the MiVoice 5300 Digital Phone firmware into the MiVoice 5000 Server storage directory
- Creating the MiVoice 5300 Digital Phone groups to be updated by A5000 MiVoice 5000 Server.

**Note : MiVoice 5300 Digital Phones are updated in groups of 20 terminals. Each group contains some MiVoice 5300 Digital Phones of the same gateway. There are as many groups as there are gateways and as many groups as required for a gateway. The terminals are assigned to groups at random (they are not all on the same equipment).**

- Update request transmitted to gateways
- Transferring the MiVoice 5300 Digital Phone firmware to the gateway storage directory
- Automatic update of terminals MiVoice 5300 Digital Phone by the gateways.

**Note : MiVoice 5300 Digital Phone groups are updated simultaneously on each gateway.**

**ATTENTION : It takes approximately 20 minutes to update a group. MiVoice 5300 Digital Phones restart even during a call in order to be updated. Mivoice 5300 Digital Phones are not operational during the update phase. In case of update error, the MiVoice 5300 Digital Phone concerned restarts its update in the next group. The groups are updated one after the other, until each MiVoice 5300 Digital Phone is updated. The terminals in the first group remain operational while the first group is being updated.**

# 7.15 ADDITIONAL TMA FUNCTIONS

## 7.15.1 DOWNLOADING FILES INDIVIDUALLY

**ATTENTION : This feature only applies to Mitel 6000 SIP Phone and MiVoice 5300 IP Phone.**

As of R3.1C, a new feature is used to download an individual file to the FTP server(s). This feature is used, in particular, to provide on the FTP server(s) with the template files (Mitel 6000 SIP Phone.cfg) used by Mitel 6000 SIP Phones and the certificates (ca.crt) used by Mitel 6000 SIP Phones and MiVoice 5300 IP Phones when encryption is enabled and an external certificate is used.

To download a file individually, proceed as follows:

- Click the **Deployment** menu.
- Select the **Region**, **Multisite** and the terminal range (**6xxxi or 53xxip).**
- From the **List of FTP servers,** select the FTP server to which the certificate must be downloaded.
- In the **Other file** field import, by clicking **Browse**, the template file (Mitel 6000 SIP Phone.cfg) or certificate (ca.crt) to download.
- Click **Validate**.
- Enter the **Action name**.
- Indicate **the type of update**: immediate or deferred.
- Click **Validate**.
- In **Action monitoring** check that the file is correctly downloaded individually to the FTP server.

**ATTENTION : An FTP server must be selected. Only one file is authorised per provisioning operation. This file is not backed up in the TMA directories.**

**ATTENTION : Some file name checks are made:**
**- This cannot be a global data file; therefore, the name must be different from aastra.cfg (if 6xxxi range is selected) or localdb.config.ftp (if 53xxip range is selected).**
**- If configuration file encryption is activated, TMA does not allow *.cfg files to be sent to the FTP server as they will not be taken into account.**

## 7.15.2 EXPORTING THE DATA CONTAINED IN THE CONFIGURATION FILES OF MITEL 6000 SIP PHONES AND MIVOICE 5300 IP PHONES

**ATTENTION : This feature only applies to Mitel 6000 SIP Phone and MiVoice 5300 IP Phone.**

The global and specific data of terminals with a production or test software release may be exported in **.csv** format from the **Terminals configuration export** menu.

Refer to Chapter 6.21.2 à la page 186 for more information about the procedure.

- Select the **Region** and the **Multisite** concerned then the **Range** and possibly the **Model**.

The **specific site data** button is used to export in **.csv** format only the specific data of terminals in site-based production software release. This export is saved in the file **export_specific_site**. This function is used to export the specific data meant to be used by TMA-EP.

### 7.15.3 EXPORTING THE DATA CONTAINED IN INVENTORIES OF MITEL 6000 SIP PHONE, MIVOICE 5300 IP PHONE AND MIVOICE 5300 DIGITAL PHONE

The Mitel 6000 SIP Phone and MiVoice 5300 IP Phone data displayed in the inventory can be exported to a **.csv** file.

Refer to Chapter 6.21.3 à la page 186 for more information about the procedure.

- Select the **Region** and the **Multisite** concerned then the **Range** and possibly the **Model**.
- If possible, apply a filter to the current inventory based on:
  - The subscription community
  - The subscription reference site
  - The terminal subscription number
  - The terminal IP address
  - The terminal software release (production, test release, etc.)
  - The terminal global data index
  - The terminal specific data index
  - The terminal MAC address

**Note : The joker * may be applied to the parameters Number, IP address and Mac address by placing them at the end of the parameter value.**

**Note : The export function is also available from Action monitoring.**

### 7.15.4 PRINTING THE DATA CONTAINED IN INVENTORIES OF MITEL 6000 SIP PHONE, MIVOICE 5300 IP PHONE AND MIVOICE 5300 DIGITAL PHONE

The terminal data displayed in the inventory can be printed out.

Refer to Chapter 6.21.4 à la page 187 for more information about the procedure.

- Select the **Region** and the **Multisite** concerned then the **Range** and possibly the **Model**.

**Note : The print function is also available from Action monitoring.**

### 7.15.5 EVENT LOG

The event log is basically used to check the status of the following actions:

- Deployment
- Terminal software release update
- Terminal global data update
- Terminal specific data update

Each action is identified by the following information:

- The **Date** on which the action was started
- The **Time** the action was started
- The **Multisite** concerned by the action
- The name of the **User** who started the action
- The type of**Action** concerned

- The **Name of the action** concerned
- The **Status** of the action concerned

The information displayed may be filtered with certain criteria:

- Click the menu 

.
- Select any of the following:
  - **Region**
  - **Multisite**
  - **User**
  - **Action**
  - **Status**
  - **Start date** and **End date.**

**Note : Clicking the icon opens the calendar so the start and end dates can be selected directly.**

- Click **Filter** for the filtering criteria to become effective.

**Note : Clicking Initialise deletes the filter criteria and displays the entire information.**

In case of operation error, the events log is used to identify the cause of the error: The following cases are taken into account:

- Network problem: no response to PING (problem accessing the MiVoice 5000 PBX),
- APACHE problem: HTTPS request timed out (problem accessing the MiVoice 5000 PBX web server),
- "MMC" service is stopped (problem accessing the MiVoice 5000 PBX MMC),
- Incorrect "login/password" (problem authenticating to the MiVoice 5000 PBX),
- Problem while sending the ".csv" file (problem sending files to the MiVoice 5000 PBX),
- Errors while sending the terminal update request: error codes are logged, but the error is not interpreted (MMC request problem (error code xx) on the MiVoice 5000 PBX).

### 7.15.6 DELETING A SOFTWARE RELEASE

This function deletes a software release installed in TMA.

The deletion is only possible if the software release is not configured as the deployment or test software release.

Proceed as follows:

- Click the menu 

.
- Select the **Region** and **Multisite** concerned then the series.

**Note : TMA retrieves the configuration of the managed regions, multi-sites and sites from MiVoice 5000 Manager.**

- Click **Change**.
- Click the link **Delete a software version**:

- select the version to delete then click **Confirm**.

The selected software release is deleted from TMA.

**Note : The selected software release is not deleted by TMA from the external FTP server storage directory. This operation must be performed manually on the external FTP server.**

## 7.15.7 IPBX CONFIGURATION

### *7.15.7.1 Managing tables*

This procedure is used to erase the data concerning the operations previously performed by TMA, saved in the tables of all the multi-site systems (as of R5.2 SP1). These tables contain, among others, information about the terminal release and index of the global configuration file in nominal mode and test mode, as well as information about FTP servers.

This procedure must be used in the following cases:

- While changing to TMA-EP mode (See the TMA-EP operating manual (AMT/PTD/TR/0027*)
- While returning to TMA mode (See the TMA-EP operating manual (AMT/PTD/TR/0027*)
- While stopping the terminal service (TMA).

The procedure to use is as follows:

- In the TMA-EP application, select the **iPBX configuration** menu.
- Select the region and multi-site configuration concerned.
- Select the site on which the TDW tables must be reset.
- Tick the terminal range(s) on which to perform the reset.
- Click **Reset tables** then confirm the iPBX table configuration reset when the warning message is displayed.
- Check in the events log that this operation is taken into account.

### *7.15.7.2 Managing the integrated FTP server*

This procedure is used to implement the previously described table management procedure on all ranges, but also to delete the content of the integrated FTP areas on a MiVoice 5000 system.

This procedure must be used if you wish to define, in the integrated TMA on a MiVoice 5000 Manager, an integrated FTP server on a MiVoice 5000 system, and if, depending on the prior configuration of this system, some links may exist in this latter's FTP areas.

This procedure only applies to systems as of R6.3.

- Select the **iPBX configuration**.
- Select the site.
- In the **integrated FTP server** part
- if the selected site is a cluster site, select **node** (seen in the cluster server as node).
- Otherwise, the list of nodes is empty.
- Click **Clean integrated FTP serve**r area to confirm the table reset and the deletion of the content of the FTP area.
- Check in the events log that this action has been taken into account.

## 7.16 PROGRAMMING THE SYSTEM KEYS FOR MITEL 6000 SIP PHONES (TEMPLATE MANAGEMENT)

The keys of Mitel 6000 SIP Phones are divided into two categories: system keys and programmable keys.

In addition to the configuration of terminal Mitel 6000 SIP Phone keys, possible on Web Admin **Menu Telephony service > Subscribers > Terminals and Applications > 6xxxi keys**, TMA completes the possibilities to program the **System** keys (speed-dial for example).

The programming for these **System** keys will be generally applied by terminal model:

- 6863 SIP,
- 6865 SIP
- 6867 SIP,
- 6869 SIP,
- 6873 SIP,
- 6710 SIP,
- 6730 SIP,
- 6731 SIP,
- 6735 SIP,
- 6737 SIP,
- 6739 SIP,
- 6753 SIP,
- 6755 SIP,
- 6757 SIP



**Note : This type of programming is not applicable to terminal 6751 SIP (no programmable key on this model).**

The programming for these **System** keys must be indicated, for each terminal type, in a specific pre-formatted file called "**TEMPLATE**". These files are available in the **sip_sets_tma** directory of the MiVoice 5000 DVD.

**Procedure:**

- Create a file from the model provided and save it respecting the syntax **modele.cfg** (example 6755i.cfg).
- From **Deployment** Menu via the parameter Other File, successively download all the **Templates** files concerned to the FTP servers.



**ATTENTION : The terminal must be restarted for the template file or certificate to be taken into account.**

## 7.17 TROUBLESHOOTING SOLUTIONS

### 7.17.1 INVENTORY IS NOT UPDATED AUTOMATICALLY

If the information contained in the TMA inventory is not updated automatically, the data on the site concerned must be imported from MiVoice 5000 Manager in the following cases:

- If only the data of a MiVoice 5000 Server or Mitel 5000 Gateways system is restored,
- If the data of and code of a MiVoice 5000 Server or Mitel 5000 Gateways system is restored,

- In case of switchover to the inactive partition of a MiVoice 5000 Server or Mitel 5000 Gateways system.

This import guarantees the consistency of the information about the traps stored both in MiVoice 5000 Server or Mitel 5000 Gateways systems and in the MiVoice 5000 Manager database.

To import data from the site concerned into MiVoice 5000 Manager, proceed as follows:

- Start TMA from the MiVoice 5000 Manager application in a Windows client PC:
  - In the Start menu, click Programs > Mitel > Parkclient.
  - Enter the login and password assigned by the administrator: the welcome window opens on the MiVoice 5000 Manager welcome screen.
  - Click the **Administration** menu then the **Network topology** menu.
  - Select the multi-site concerned then the **Configuration** menu.
  - In the area **Import a new site in the multisite,** select the site concerned then click **Import**.
  - Do not tick **Import site local directory data**.
  - Click **Start**.

# 8 MANAGING A HETEROGENEOUS NETWORK WITH TMA HOSTED BY MIVOICE 5000 MANAGER

Refer to the TMA-EP operating manual AMT/PTD/TR/0027*

# 9 CONFIGURING THE DHCP SERVER INTEGRATED MIVOICE 5000 SYSTEMS

The DHCP server integrated into Mitel 5000 Gateways and MiVoice 5000 Server systems allows the management of the following Mitel terminals:

- MiVoice 5300 IP phones,
- Mitel 6000 SIP Phones
- IP DECT base station
- Mitel DECT base station
- WIFI terminal 312i
- Terminals i7xx
- Blustar 8000i



**ATTENTION : As of R6.2, the integrated DHCP server also responds to requests from devices without Vendor Class (servers, PC, etc.) and from devices with specific Vendor Classes different from those already taken into account by the integrated DHCP server (see above). In this latter case, some template files describing the Vendor Class settings associated with these devices may be imported into the integrated DHCP server.**

The DHCP server can deliver IP addresses for one or more subnets.

The DHCP server can supply data to Mitel terminals connected to different systems (multi-site configuration) within the limit of the planned capacity.

Some examples of the architecture associated with the DHCP server integrated into Mitel 5000 Gateways are provided in Chapitre 14 : Appendix 3.



**ATTENTION : The DHCP server integrated into Mitel 5000 Gateways is limited to configurations with at most 500 IP terminals. If the DHCP and FTP servers integrated into Mitel 5000 Gateways are used at the same time, the configuration of the integrated DHCP server is limited to 200 IP terminals.**



**ATTENTION : The DHCP server integrated into MiVoice 5000 Server is limited to configurations with at most 500 IP terminals and 4 subnets.**

**As of R6.2, in a redundant MiVoice 5000 Server configuration, the DHCP server integrated into MiVoice 5000 Server systems is available. In this case, the virtual IP address can be configured in the integrated DHCP server.**

## 9.1 DHCP SERVICE HOME PAGE

From the web browser, connect to the system's MiVoice 5000 Web Admin.

- Click the **DHCP Service** menu.

The DHCP Service configuration MMI appears.

The following menus are accessible in the left column:

| | |
|---|---|
| Home | : This menu is used to return to the Web Admin home page. |
| DHCP - Creation | : This menu is used to define a new DHCP configuration. |
| DHCP - Managing | : This menu is used to modify the current DHCP configuration. |
| Templates management | : This menu is used to manage a new device by importing a template file in XML format. |
| Restore - Delete | : This menu is used to restore or delete an archive*. |
| Restart the DHCP service | : This menu is used to restart the DHCP service**. |
| Status of the DHCP service | : This menu displays the current status of the DHCP service. |
| Display of DHCP settings | : This menu displays the (the current and operational) file dhcpd.conf in HTML format. |
| Display of DHCP leases | : This menu displays the file dhcpd.leases in HTML format. |

* Restoring an archive allows you to work on a new configuration but the working configuration remains valid.

** The current configuration becomes operational.

## 9.2 CREATING A NEW DHCP CONFIGURATION

- From the **DHCP Service** configuration MMI, click the menu **DHCP - Create**.

  A confirmation message appears: click the **Validate** button to confirm the overwriting of the current configuration data and the creation of a new, current configuration.

- The general parameters definnition window opens.

**Note : Store the current configuration before overwriting it.**

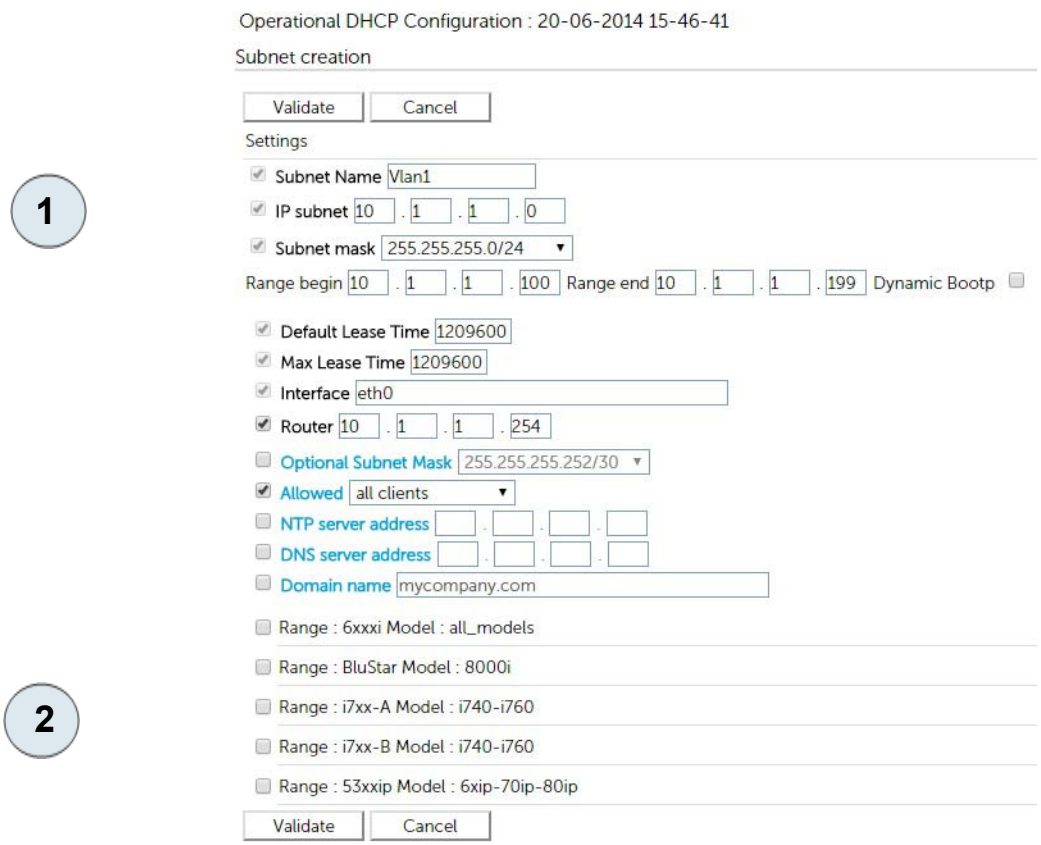
## 9.3 CONFIGURING THE GENERAL PARAMETERS OF THE DHCP SERVER

- Leave the default values of the DHCP server general parameters:
  - **Type of DNS update***: none
  - **The network exercises authority***: yes (ticked)
  - **Ignore** *: not selected (by default, all the requests are accepted).
  - **Local address:** for a redundant configuration, this parameter indicates the virtual IP address to which the integrated DHCP server will send its DHCP messages.
  - **Server ID**: in a redundant configuration, this parameter is used to indicate the virtual IP address used to identify the DHCP server.

**Note : * The meaning of these parameters is indicated in Appendix 2.**

- Select the Mitel terminal(s) to be configured in the DHCP server by ticking the appropriate box.
- Click **Add** (in the **Subnet** column on the top right side) to create a subnet.

The following configuration window opens:




1 The upper part of the MMI defines the standard network parameters associated with the subnet in question.

2 The lower part of the MMI defines the specific network parameters of each type of terminal associated with the subnet in question. The terminal types concerned are:

- Mitel 6000 SIP Phones, models 6730 SIP, 6731 SIP, 6751 SIP, 6753 SIP, 6755 SIP and 6757 SIP (version 2.1 and later)
- Mitel 6000 SIP Phone, model 6739i (version 3.0 and later)
- Mitel 6000 SIP Phone, models 6735 SIP and 6737i (version 3.2 and later)
- Mitel 6000 SIP Phone, models 6863 SIP, 6865 SIP, 6867 SIP and 6869 SIP (version 3.3 and later)
- Mitel 6000 SIP Phone, model 6873 SIP (version 4.2 and later)
- Mitel 6000 SIP Phone all_models: all the Mitel 6000 SIP Phone models are configured in the same way.
- Blustar 8000i (version 4.0 and later)
- Blustar, Vpn model
- MiVoice 5300 IP Phone, models 60ip/70ip/80ip (version V2.10.25 and later)
- MiVoice 5300 IP Phone, model 61ip (version 4.0 and later)
- IP DECT terminals (versions 1.04 , 1.5, and 2.1)
- SIP DECT terminals (version 4.0 and later)

- WIFI terminals, model 312i (version 1.09 and later)
- Terminals i7xx-A, model i740/i760 (version < 5.3)
- Terminals i7xx-B, model i740/i760 (version > 5.3)
- Range TA7102i
- Range UC360

The terminal types are associated with the profiles whose unique identifier is the terminal's supplier class. This supplier class is the discriminating condition displayed above in the MMI used to filter and accept only DHCP requests from this terminal.

**ATTENTION : If you want the integrated DHCP server to also respond to requests from devices without Vendor Class (servers, PC, etc.), set the parameter *Allow* to *All clients*.**

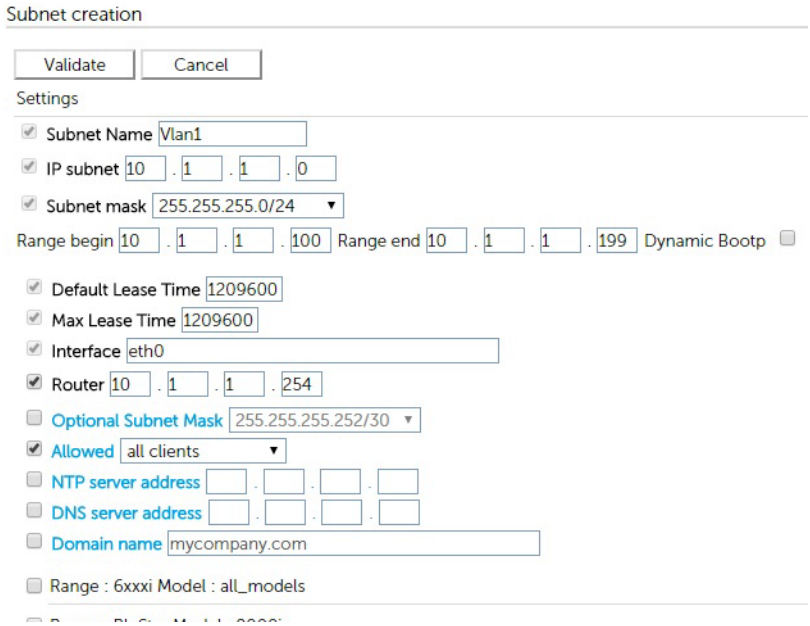
.

**Note : For Mitel 6000 SIP Phones, you may use either all_models, or you can select the models one by one.**

**Note : Refer to document AMT/PTD/PBX/0137* for more information on how to set Blustar 8000i to VPN mode.**

**ATTENTION : For the same DECT network, DECT IP and DECT SIP are exclusive.**

## 9.4 CONFIGURING THE STANDARD PARAMETERS OF THE SUBNET




Enter the following parameters:

- Subnet name: indicate, for instance the membership VLAN or the actual name
- Subnet IP: enter the sub-network IP address.
- Subnet mask: select the subnet mask.
- Start of segment: enter the first IP address available in the segment.
- End of segment: enter the last IP address available in the segment.
- Default lease duration: 14 days by default (this value is expressed in seconds and can be modified if necessary). Lease assigned to the client who has not asked for a specific duration
- Max. lease duration: 14 days by default (this value is expressed in seconds and can be modified if necessary). Maximum duration of a lease assigned to a client who has asked for a specific duration
- Interface: name of the network interface device of the system connected to the client LAN (by default **eth0**)

All of these parameters are necessary and obligatory (checkbox in reverse video).

The following parameters are required but may be optional depending on the client's network configuration:

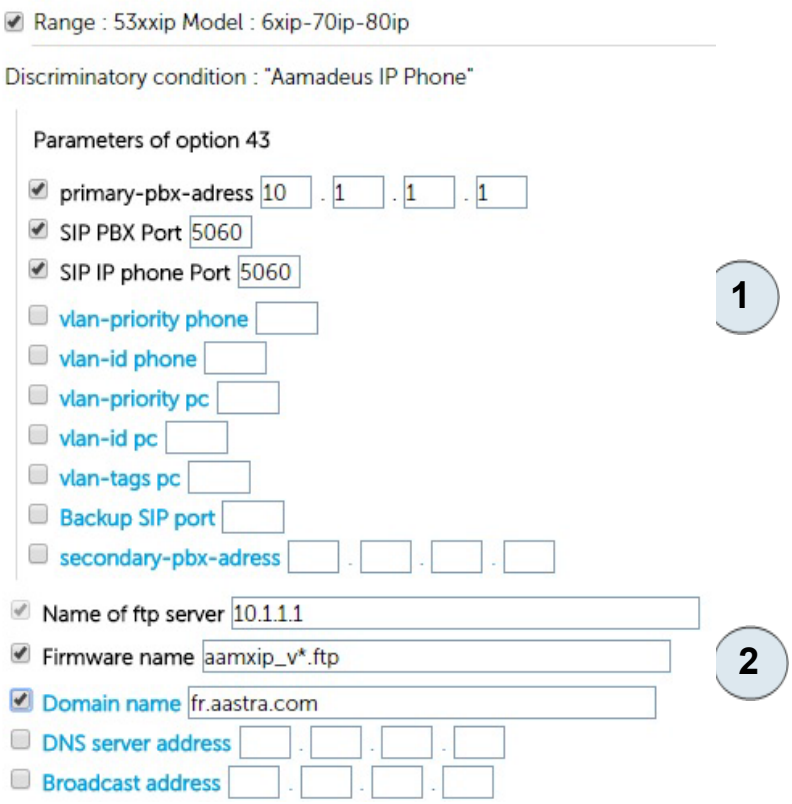
- Router: specifies the gateway (router) IP address used to leave the subnet
- Allow: used to indicate whether only known clients are managed by the integrated DHCP server or whether all the clients are managed by the integrated DHCP server. Known client must have a Vendor Client defined with some associated specific parameters. New clients may be managed via the Template management menu. These new clients must be associated with a new Vendor Class.
- Optional subnet mask*
- NTP server address*
- DNS server address*
- Domain name*.

**Note : * The meaning of these parameters is indicated in Appendix 2. If these parameters are defined, the values defined are the same for all the clients without Vendor Class.**

## 9.5 DEFINING THE SPECIFIC SUBNET PARAMETERS FOR MIVOICE 5300 IP PHONES

Tick **53xxip** range if any of the following terminal models is available on the subnet in question and must be managed by the integrated DHCP server:

- 5360 IP (version V2.10.25 and later)
- 5361 IP (version V4.0.x and later)
- 5370 IP (version V2.10.25 and later)
- 5380 IP (version V2.10.25 and later)




1 The upper part of the MMI defines the specific network parameters negotiated via Option 43 with MiVoice 5300 IP Phone for the subnet in question.

2 The lower part of the MMI defines the standard network parameters negotiated with MiVoice 5300 IP Phones for the subnet in question.

Enter the following parameter:

- Ftp server name: IP address of the FTP server on which the firmware and configuration files are stored. For a simplified configuration, enter the IP address of the FTP server incorporated into the Mitel 5000 Gateways or MiVoice 5000 Server.

The following specific parameters (parameters of Option 43) are optional, depending on the subnet configuration:

- primary-pbx-address: Specifies the SIP gateway main IP address
- port sip pbx: Specifies the listening SIP port of the main system
- port sip ip phone: Specifies the listening SIP port of the terminal

- vlan-priority phone: Specifies the terminal's VLAN port priority
- vlan-id phone: Specifies the VLAN ID used by the terminal's VLAN port.
- vlan-priority pc: Specifies the PC VLAN port priority
- vlan-id pc: Specifies the VLAN ID used by the PC port.
- vlan-tags pc: Specifies whether the VLAN ID marking used by the PC port is enabled (1) or not (0)
- backup sip port: Specifies the secondary IP address of the SIP gateway.
- secondary-pbx-address: Specifies the listening SIP port of the secondary system

The following standard parameters are optional, depending on the subnet configuration:

- Firmware name: aamxip_v*.ftp (value configured by default in the terminal profile)
- Domain name*
- Broadcast address*
- DNS server address*



**Note : * The meaning of these parameters is indicated in Appendix 2.**

**If these parameters are entered, they are taken into account instead of the ones defined in the global subnet parameters.**

Tick another terminal range or confirm the current configuration by clicking **Confirm.**

## 9.6 DEFINING THE SPECIFIC SUBNET PARAMETERS FOR MITEL 6000 SIP PHONE AND 8000I

**ATTENTION : For Mitel 6000 SIP Phones, you may use either all_models, or you can select the models one by one.**

Tick **6xxxi model all_models** range if any of the following terminal models is available on the subnet in question and must be managed by the integrated DHCP server:

- Model 6730 SIP, 6731 SIP, 6751 SIP, 6753 SIP, 6755 SIP and 6757 SIP (version 2.1 and later)
- Model 6739i (version 3.0 and later)
- Model 6735 SIP and 6737 SIP (version 3.2 and later)
- Model 6863 SIP, 6865 SIP, 6867 SIP and 6869 SIP (version 3.3 and later)
- Model 6873 SIP (version 4.2 and later)

**Note : If range 6xxxi, model all_models is not ticked, the terminal models can be selected one by one by ticking the terminal model of the Mitel 6000 SIP Phone range concerned.**

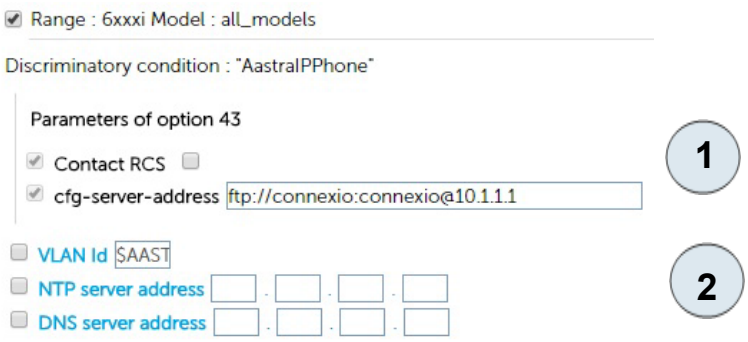
Tick **Blustar model 8000i**, if the following terminal model is available on the client's LAN and must be managed by the DHCP server:

- 8000i (version 4.0 and later).

Tick **Blustar, Vpn model** if a remote Blustar 8000i must be managed by the integrated DHCP server via an integrated VPN access on the MiVoice 5000 Server.

**Note : The integrated VPN service is not available on Mitel 5000 Gateways.**

No matter the Mitel 6000 SIP Phone model selected, the configuration is identical.




1 The upper part of the MMI defines the specific network parameters negotiated via Option 43 with Mitel 6000 SIP Phones for the subnet in question.

2 The lower part of the MMI defines the standard network parameters negotiated with Mitel 6000 SIP Phones for the subnet in question.

Enter the following specific parameters (parameters of Option 43):

- cfg-server-address: IP address of the FTP server on which the firmware and configuration files are stored. For a simplified configuration, enter the IP address of the FTP server incorporated into the Mitel 5000 Gateways or MiVoice 5000 Server.

**ATTENTION : The input is predefined (login and password) and must be completed after the character @ with the FTP server IP address: ftp://connexio:connexio@10.1.1.1.**

- Contact RCS: the parameter used to disable the RCS (Redirection & Configuration Server): If this parameter is not ticked, RCS is disabled.

**Note : This parameter is not available for the Blustar range.**

The following standard parameters are optional, depending on the client's network configuration:

- VLAN id: Specifies the VLAN ID used by the terminal’s VLAN port.
- NTP server address*
- DNS server address*

**Note : * The meaning of these parameters is indicated in Appendix 2.**

**If these parameters are entered, they are taken into account instead of the ones defined in the global subnet parameters.**

Tick another terminal range or confirm the current configuration by clicking **Confirm.**

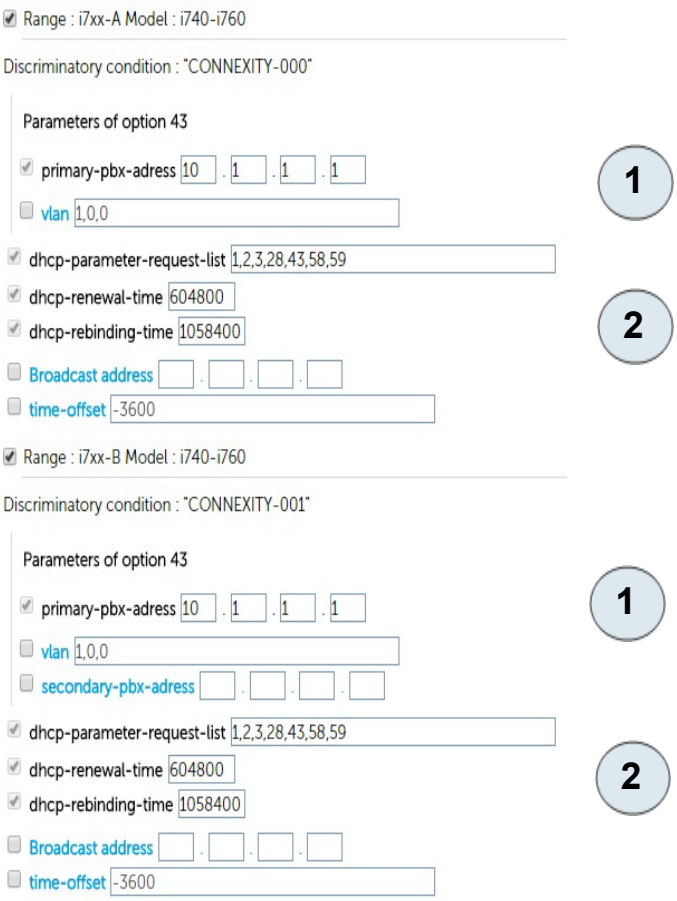
## 9.7 DEFINING THE SPECIFIC SUBNET PARAMETERS FOR TERMINALS I7XX

Tick **i7xx-A** range if any of the following terminal models is available on the subnet in question and must be managed by the DHCP server:

- i740 version < V5.3
- i760 version < V5.3

Tick **i7xx-B** range if any of the following terminal models is available on the client's LAN and must be managed by the DHCP server:

- i740 version > V5.3
- i760 version > V5.3




1 The upper part of the MMI defines the specific network parameters negotiated via option 43 with terminals i7xx for the subnet in question.

2 The lower part of the MMI defines the standard network parameters negotiated with terminals i7xx for the subnet in question.

Enter the following parameters:

- primary-pbx-address: Main system IP address. For a simplified configuration, enter the IP address of the Mitel 5000 Gateways.
- dhcp-renewal-time: defines the lease renewal periods (in unicast mode). By default, these periods are equal to 50% of the lease duration. If the default lease duration is modified, you have to adjust this value.
- dhcp-rebinding-time: defines the ultimate lease renewal periods (in broadcast mode). By default, these periods are equal to 87.5% of the lease duration. If the default lease duration is modified, you have to adjust this value.
- dhcp-parameter-request-list: defines the list of parameters that the DHCP server will deliver to terminals i7xx

The following specific parameters are optional, depending on the subnet configuration:

- vlan

Format: “b, iiii, p”

  - “b” is the VLAN status: 0 for disabled, 1 for enabled (marking of frames 802.1Q).
  - “iiii” is the VLAN ID, between 1 and 4094.
  - “p” is the value of the priority field (“0” to “7”).

If the VLAN is disabled, the “iiii” and “p” fields are optional.

- secondary-pbx-address: Secondary system IP address. This parameter is only available for the i7xx-B range (function not available in V5.1A).

The following standard parameters are optional, depending on the subnet configuration:

- time-offset*
- Broadcast address*



**Note : * The meaning of these parameters is indicated in Appendix 2.**

Tick another terminal range or confirm the current configuration by clicking **Confirm.**

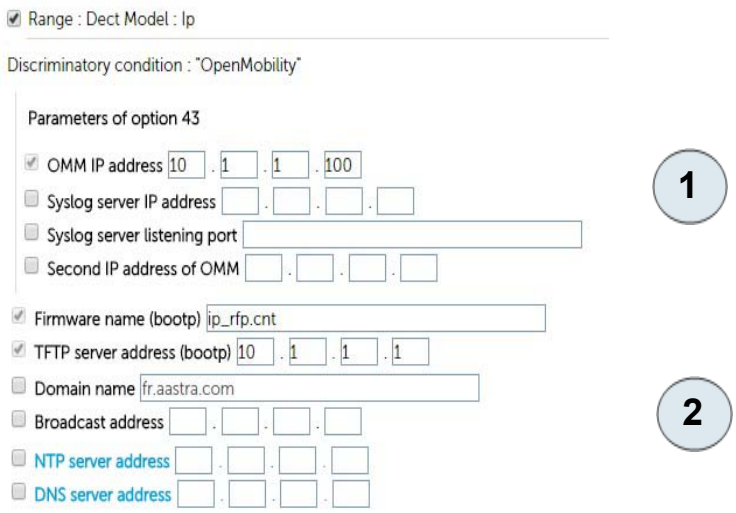


**ATTENTION : The download server address parameter is defined by default in the global parameters of the DHCP server for terminals i7xx. The value associated with this parameter is: 0.0.0.0:9410.**

## 9.8 DEFINING THE SPECIFIC SUBNET PARAMETERS FOR THE DECT/IP BASE STATIONS (RFPS)

Tick the **IP DECT** range if any of the following terminal models is available on the subnet in question and must be managed by the DHCP server:

- **IP DECT base station.** This allows old Mitel RFP / RFP-L 32, 34 or 42 to be managed on a DECT network hosting Mitel OMM 2.1 or earlier (1.4 or 1.5) on any of these RFPs.




1 The upper part of the MMI defines the specific network parameters negotiated via option 43 with IP DECT base stations for the subnet in question.

2 The lower part of the MMI defines the standard network parameters negotiated with IP DECT base stations for the subnet in question.

Enter the following parameters:

- Mitel OMM IP address IP address of the base station hosting the Mitel OMM software 2.1 or earlier that manages the Mitel SIP DECT STIMULI signalling interface with the SIP gateway incorporated into the Mitel 5000 Gateways or MiVoice 5000 Server.

**ATTENTION : An IP address reservation must be declared for the IP DECT base station hosting Mitel OMM software 2.1. IP address reservation is defined via the host creation MMI (see “Defining the specific subnet parameters for terminals TA7102i” on page 262).**

**ATTENTION : If the base station version is 1.04, an IP address reservation must be declared for all the other IP DECT base stations available in the subnet in question. IP address reservation is defined via the host creation MMI (see “Defining the specific subnet parameters for terminals TA7102i” on page 262). As from version 1.5, these reservations are no longer necessary.**

- Firmware name: name of the file downloaded to each base station.
- TFTP (bootp) server address: IP address of TFTP server For a simplified configuration, enter the IP address of the TFTP server incorporated into the Mitel 5000 Gateways or MiVoice 5000 Server.

The following specific parameters are optional, depending on the subnet configuration:

- Syslog server IP address
- Syslog server listening port
- Second Mitel OMM IP address (managed as from version 1.5)

The following standard parameters are optional, depending on the subnet configuration:

- Domain name*
- Broadcast address*
- NTP server address*
- DNS server address*

**Note : * The meaning of these parameters is indicated in Appendix 2.**

**If these parameters are entered, they are taken into account instead of the ones defined in the global subnet parameters.**

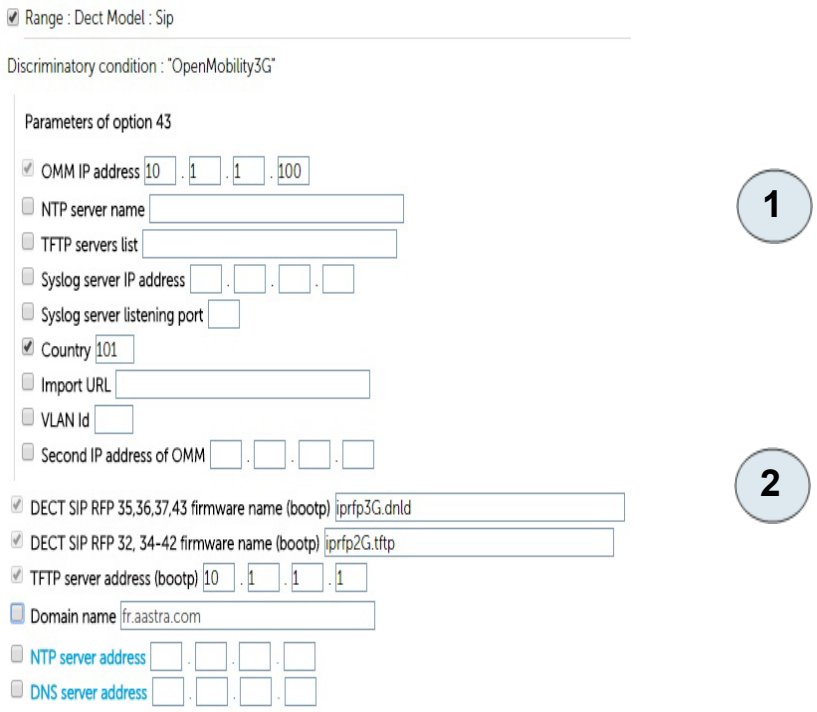
**ATTENTION : The parameter for public option 224 is defined by default in the DHCP server's global parameters for IP DECT base stations. The value associated with this parameter is: OpenMobility.**

Tick another terminal range or confirm the current configuration by clicking **Confirm**.

## 9.9 DEFINING THE SPECIFIC SUBNET PARAMETERS FOR MITEL DECT/ SIP BASE STATIONS (RFPS)

Tick the S**IP DECT** range if any of the following terminal models is available on the subnet in question and must be managed by the DHCP server:

- S**IP DECT base station.** This allows new Mitel RFP / RFP-L 35, 36 or 43 to be managed on a DECT network hosting Mitel OMM (1.4 or later) on any of these RFPs. Old Mitel RFP / RFP-L 32, 34 or 42 can also be managed when used together on this same network with a new RFP hosting Mitel OMM 4.0.




**1** The upper part of the MMI defines the specific network parameters negotiated via option 43 with Mitel SIP DECT base stations for the subnet in question.

**2** The lower part of the MMI defines the standard network parameters negotiated withMitel S IP DECT base stations for the subnet in question.

Enter the following parameters:

- Mitel OMM IP address IP address of the Mitel RFP / RFP-L 35, 36, 37 or 43 hosting the Mitel OMM software 4.0 or later that manages the functional Mitel SIP DECT signalling interface with the SIP gateway incorporated into the Mitel 5000 Gateways or MiVoice 5000 Server.

**ATTENTION : An IP address reservation must be declared for the Mitel SIP DECT base station hosting Mitel OMM software 4.0. IP address reservation is defined via the host creation MMI (see “Defining the specific subnet parameters for terminals TA7102i” on page 262).**

- Name of RFP 35,36,37,43 (bootp) SIP DECT firmware: **iprfp3G.dnld** (default name of the Mitel OMM 4.0 firmware available in the integrated TFTP server storage directory)
- Name of RFP 32,34,42 (bootp) SIP DECT firmware: **iprfp2G.tftp** (default name of the firmware used by the old radio fixed parts in the integrated TFTP server storage directory).

**Note : The configuration of the 2 firmware allows new and old radio fixed parts to be used together on the same OMM 4.0 DECT network.**

- TFTP server address (bootp): address of the integrated TFTP server or of an external TFTP server whose storage directory contains the firmware **iprfp3G.dnld and iprfp2G.tftp** For a simplified configuration, enter the IP address of the TFTP server incorporated into the Mitel 5000 Gateways or MiVoice 5000 Server.

The following specific parameters are optional, depending on the subnet configuration:

- NTP server name
- TFTP server list (list of additional TFTP servers)
- Syslog server IP address
- Syslog server listening port (514 by default)
- Country (country code for configuring tones: 101 for France)
- Import url (allows a configured Mitel OMM database to be imported automatically)
- VLAN ID (used to specify the RFP membership VLAN)
- Second Mitel OMM IP address (standby Mitel OMM IP address in a redundant Mitel OMM configuration)

The following standard parameters are optional, depending on the subnet configuration:

- Domain name*
- NTP server address*
- DNS server addresses*.

**Note : * The meaning of these parameters is indicated in Appendix 2.**

**If these parameters are entered, they are taken into account instead of the ones defined in the global subnet parameters.**

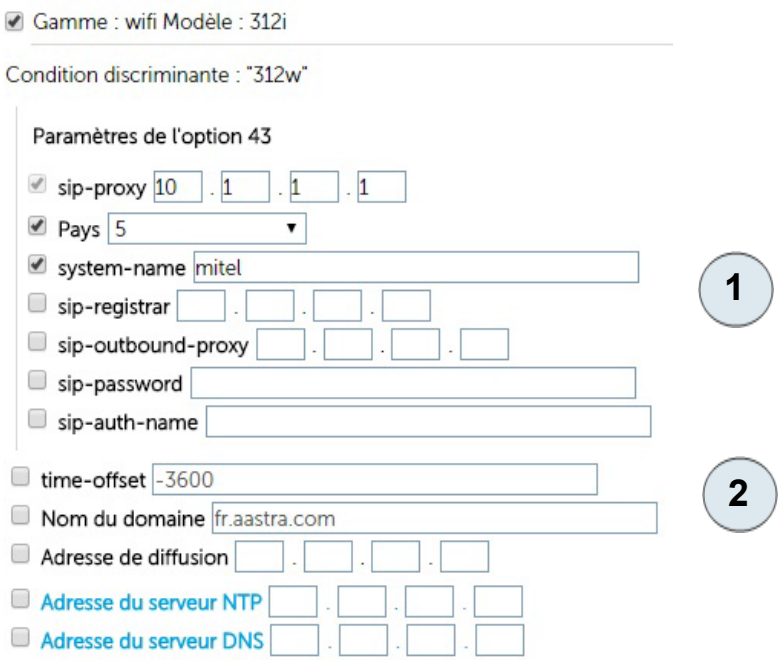
**ATTENTION : The parameter for public option 224 is defined by default in the DHCP server's global parameters for Mitel SIP DECT base stations. The value associated with this parameter is: SIP-DECT OpenMobility.**

Tick another terminal range or confirm the current configuration by clicking **Confirm.**

## 9.10 DEFINING THE SPECIFIC SUBNET PARAMETERS FOR TERMINALS 312I

Tick the **Wifi 312i** range if any of the following terminal models is available on the subnet in question and must be managed by the DHCP server:

- WIFI terminals 312i version 1.09 and later




1 The upper part of the MMI defines the specific network parameters negotiated via option 43 with terminals 312i for the subnet in question.

2 The lower part of the MMI defines the standard network parameters negotiated with terminals 312i for the subnet in question.

Enter the following parameters:

- sip-proxy: SIP gateway IP address. For a simplified configuration, enter the IP address of the Mitel 5000 Gateways or MiVoice 5000 Server.

The following specific parameters are optional, depending on the subnet configuration:

- Country code (options list)
- system-name: SIP account name
- sip-registrar: Registrar address if different from the SIP gateway (not used with the MiVoice 5000 solution)
- sip-outbound-proxy: Outgoing proxy address if different from the SIP gateway (not used with the MiVoice 5000 solution)
- sip-password: SIP user password (not used with the MiVoice 5000 solution)
- sip-auth-name: (not used with the MiVoice 5000 solution)

The following standard parameters are optional, depending on the subnet configuration:

- time-offset*
- Domain name*
- NTP server address*
- DNS server address*
- Broadcast address*.

**Note : * The meaning of these parameters is indicated in Appendix 2.**

**If these parameters are entered, they are taken into account instead of the ones defined in the global subnet parameters.**

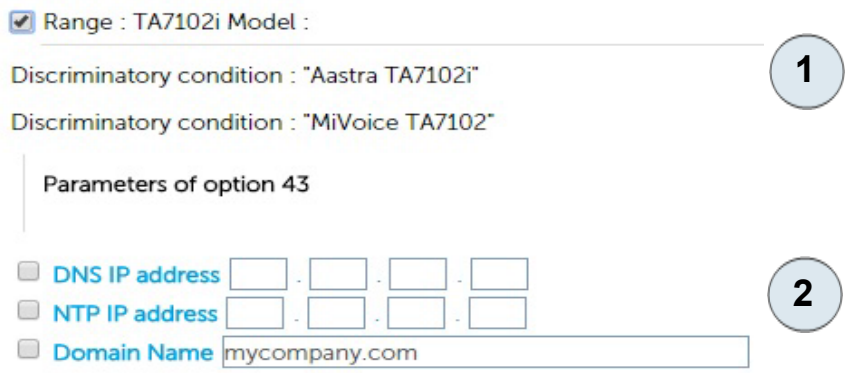
**ATTENTION : The SIP User ID parameter (SIP subscription number defined in the Mitel 5000 Gateways system associated with terminal 312i) is declared in the host creation menu (see “Defining the specific subnet parameters for terminals TA7102i” on page 262 ). An IP address reservation must be declared for all terminals 312i available in the subnet in question.**

Tick another terminal range or confirm the current configuration by clicking **Confirm**.

## 9.11 DEFINING THE SPECIFIC SUBNET PARAMETERS FOR TERMINALS TA7102I

Tick **TA7102i** range if any of the following terminal models is available on the subnet in question and must be managed by the DHCP server:

- Terminal TA7102i




1 The upper part of the MMI defines the specific network parameters negotiated via option 43 with terminals **TA7102i** for the subnet in question.

2 The lower part of the MMI defines the standard network parameters negotiated with terminals TA7102i for the subnet in question.

The following standard parameters are optional, depending on the subnet configuration:

- NTP server address*
- Domain name*
- DNS server address*

**Note : * The meaning of these parameters is indicated in Appendix 2.**

**If these parameters are entered, they are taken into account instead of the ones defined in the global subnet parameters.**

**ATTENTION : Terminal TA7102i can be configured via a Web access:**

- **Login: admin/administrator or public/ (empty)**
- **The configuration file is downloaded via http.**

Tick another terminal range or confirm the current configuration by clicking **Confirm**.

## 9.12 DEFINING THE SPECIFIC SUBNET PARAMETERS FOR TERMINALS 6900 IP PHONES,UC360 AND 5304 PHONE

Tick Range: Mitel IP Phone: 6900 (Minet), UC360, 5304 Model: all_models if any of the following terminal models is available on the subnet in question and must be managed by the DHCP server:




1 The upper part of the MMI defines the specific network parameters negotiated via option 43 with terminals 6900 IP phones, UC360 and 5304 Phonefor the subnet in question.

2 The lower part of the MMI defines the standard network parameters negotiated with terminals for the subnet in question.

Enter the following parameter:

- Configuration server: IP address of the server on which are stored the configuration files required to operate terminal UC360. This is an ftp, tftp, http or https.type server. The VLAN ID can be configured in the configuration files. The  files are
  - MN_Generic.cfg
  - MN_@MAC;cfg.

The following standard parameters are optional, depending on the subnet configuration:

- NTP server address*
- Domain name*
- DNS server address*

**Note : * The meaning of these parameters is indicated in Appendix 2.**

**If these parameters are entered, they are taken into account instead of the ones defined in the global subnet parameters.**

Tick another terminal range or confirm the current configuration by clicking **Confirm**.

# 9.13 INCORPORATING TERMINALS 6900, UC360 AND 5304 IN THE INTEGRATED DHCP OF MIVOICE 5000

## 9.13.1 INTRODUCTION

Terminals 6900 work with two different software: MINET (default, factory mode) and SIP. MiVoice 5000 does not support terminals 6900 in MINET, but in SIP only.

Therefore, a preliminary stage is needed to update terminal 6900 in MINET to SIP.

## 9.13.2 DESCRIPTION OF DHCP

### *9.13.2.1 General overview*

Terminals 6900 offer two different vendor classes (= Option 60), depending on the downloaded software:

- If the terminal has the MINET software, the "vendor class" is "**ipphone.mitel.com**", no matter the model. In the DHCP integrated in the MiVoice 5000 solution, this corresponds to **Mitel IP Phone: 6900 (Minet), UC360, 5304**.

- If the terminal has the SIP software, the vendor class is in this format: "**AastraIPPhone69x0**" (**AastraIPPhone6920**, **AastraIPPhone6930**, **AastraIPPhone6940**). In the DHCP integrated into MiVoice 5000, this corresponds to "**6xxxi/all_models**" for global management, or respectively" **6xxxi/6920**", "**6xxxi/6930**" and "**6xxxi/6940**" for management specific to each model.



**ATTENTION : To manage terminals 6900 in the DHCP integrated into MiVoice 5000, select these device types, bearing in mind that these devices do not need the same DHCP parameters.**

This vendor class "**ipphone.mitel.com**" is also used by the following devices:

- MiVoice Conference Unit (simply called UC360),
- Mitel MiVoice 5304 IP Phone
- (simply called 5304).

These devices require the use of the following template files:

- *templateUC360.xml*: compatible for UC360 only, which describes the DHCP device "**MiVoice Conference Unit**".
- *templateIpPhoneMitel.xml*: compatible with UC360 and Mitel MiVoice 5304 IP Phone, which describes the DHCP device "**IP Phone Mitel / UC360_5304**".

As of MiVoice 5000 release R6.4, these template files are no longer necessary as all the information is contained in the new "**Mitel IP Phone: 6900 (Minet), UC360, 5304**".

In case of MiVoice 5000 upgrade, an automatic update of the DHCP configuration is envisaged only in the case below, if in the DHCP configuration:

- "**6xxxi/all_models**" is selected,
- AND "**MiVoice Conference Unit**" is not selected,
- AND "**Mitel IP Phone / UC360_5304**" is not selected.

This automatic update adds the management of the new "**Mitel IP Phone: 6900 (Minet), UC360, 5304**" by initialising the values of the parameters with those entered for "**6xxxi/ allmodels**", for each subnet managing these "**6xxxi/allmodels**" and the deletion of the template files *"templateUC360.xml"* and "*templateIpPhoneMitel.xml"*.

The other cases of upgrade, with the addition of terminals 6900, require updating the DHCP configuration manually. We will distinguish between the following cases:

- "**6xxxi/all_models**" (or specific 6xxxi models) and "**MiVoice Conference Unit**" (using the template file UC360.xml) are selected;
- "*6xxxi/all_models"* ***(or specific 6xxxi models) and "****IP Phone Mitel / UC360_5304"* ***(using the template file* templateIpPhoneMi- tel.xml*) are selected.***

### *9.13.2.2 Description of the parameters*

To manage the new "**Mitel IP Phone: 6900 (Minet), UC360, 5304**", the DHCP server integrated into MiVoice 5000 offers the following specific parameters for each subnet:

**Option 43**: character string which respects the syntax below:

```
id:ipphone.mitel.com;cfg_srvr_url=ftp://
connexio:connexio@IP;sw_tftp=@IP;cfg_uri=http://@IPserver/
path;call_srv=@IP;mode=sip;dscp=2;\0x000
```

where

- ***cfg_srvr_url=ftp://connexio:connexio@IP/***: useful for terminal 6900 in MINET mode, must contain the FTP address of the deployment directory containing the SIP software,
- ***sw_tftp=@IP***: useful for Mitel MiVoice 5304 IP Phone, TFTP address of the directory containing the files required by the terminal,
- ***cfg_uri=http://@IPserver/path***: useful for MiVoice Conference Unit, must contain the HTTP address of the directory containing the necessary files.
- ***call_srv=@IP***: useful parameter for MiVoice Conference Unit and Mitel MiVoice 5304 IP Phone, call server IP address,
- ***mode=sip***: used for Mitel MiVoice 5304 IP Phone to force operation in SIP mode, the value is already set,
- ***dscp=2***: useful for MiVoice 5304 IP Phone, for the QoS
  - **Option 132** : VLAN ID



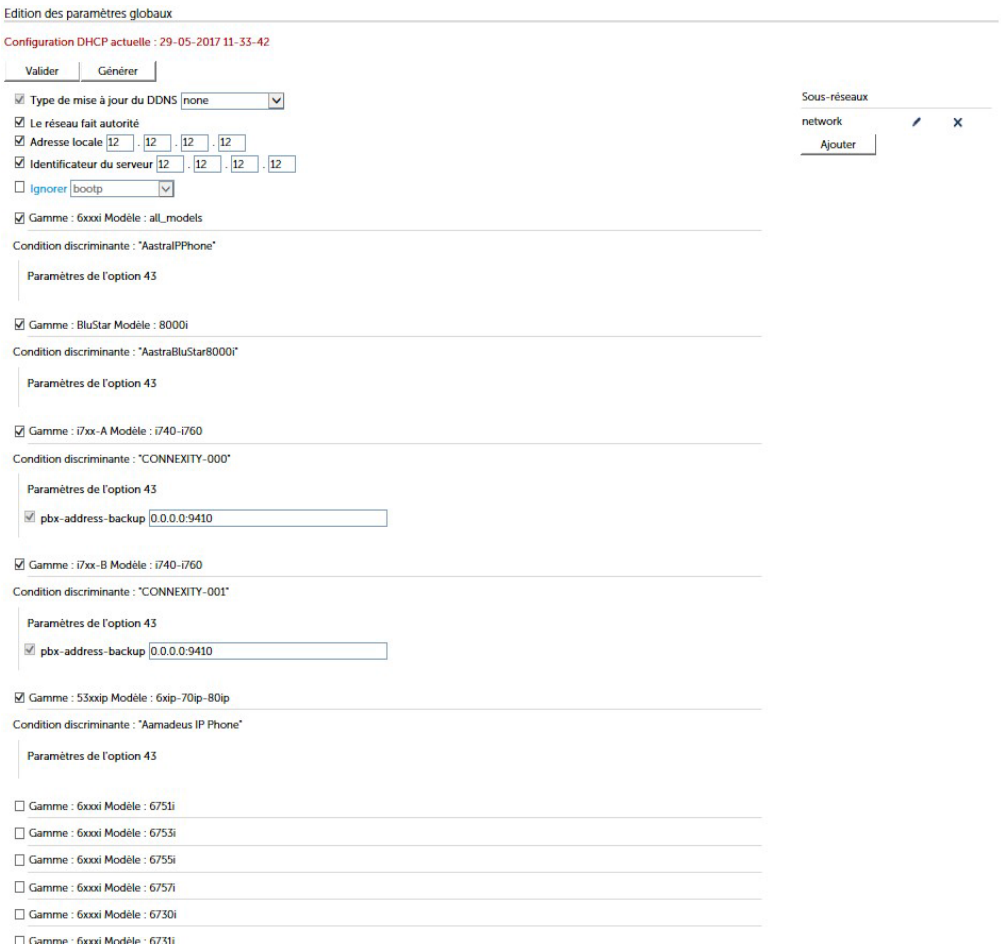
**Note : For these "ipphone.mitel.com" devices, the VLAN can also be specified in Option 43, by adding the "vlan" parameter.**

## 9.13.3 AUTOMATIC UPGRADE

### *9.13.3.1 Description*

This **automatic** upgrade is made when in the DHCP configuration:

- "**6xxxi/all_models**" is selected,
- AND **MiVoice Conference Uni**t is not selected (using the template file templateUC360.xml),
- AND **IP Phone Mitel / UC360_5304** is not selected (using the template file *templateIpPhoneMitel.xml*).

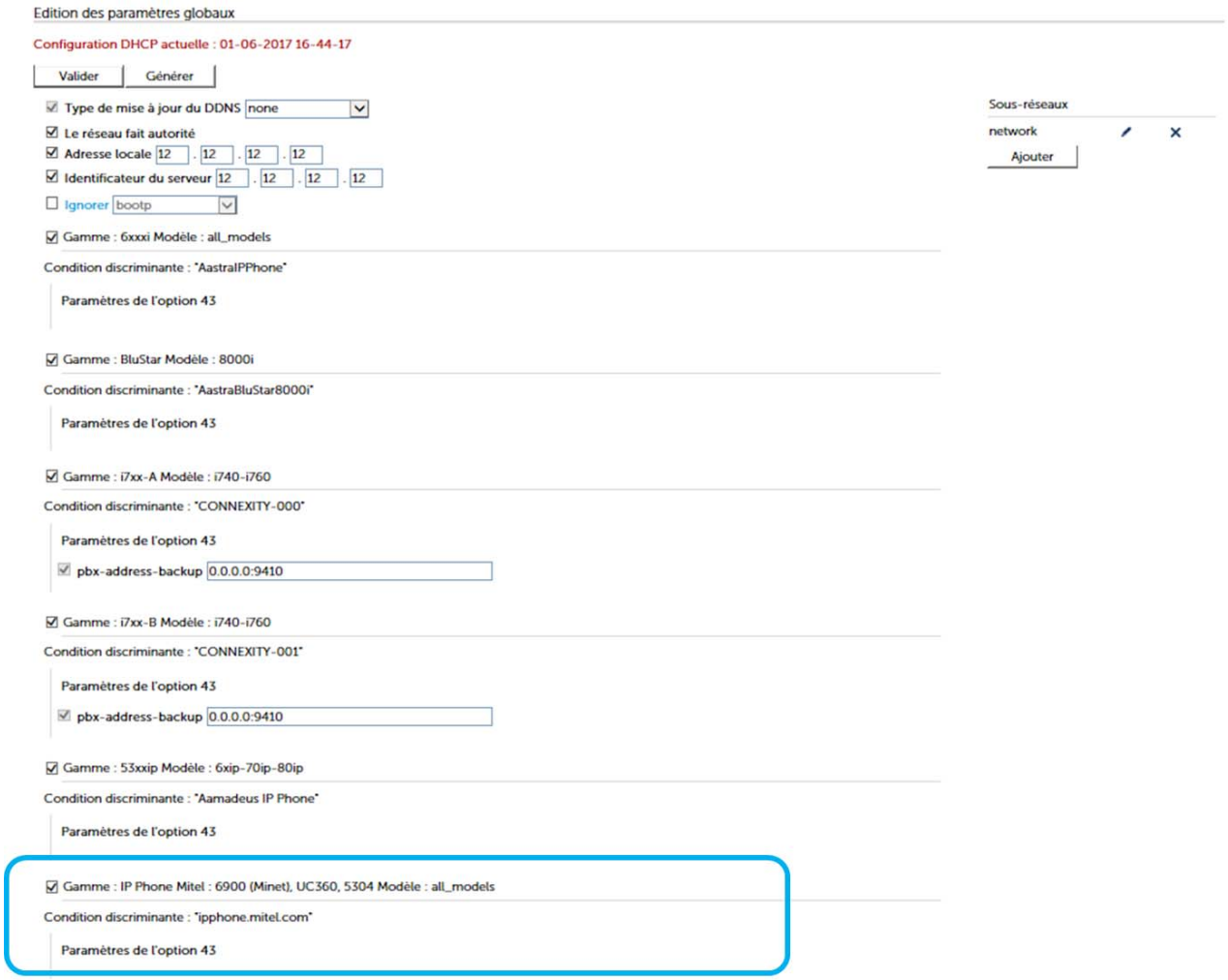



**Example of configuration concerned by automatic update**

**Note : This automatic upgrade is made when the DHCP server starts. Therefore, it does not need any action by the installer.**

### 9.13.4 RESULT

In the general parameters, "**Terminal range: Mitel IP Phone: 6900 (Minet), UC360, 5304 Model: all_models**" is selected.



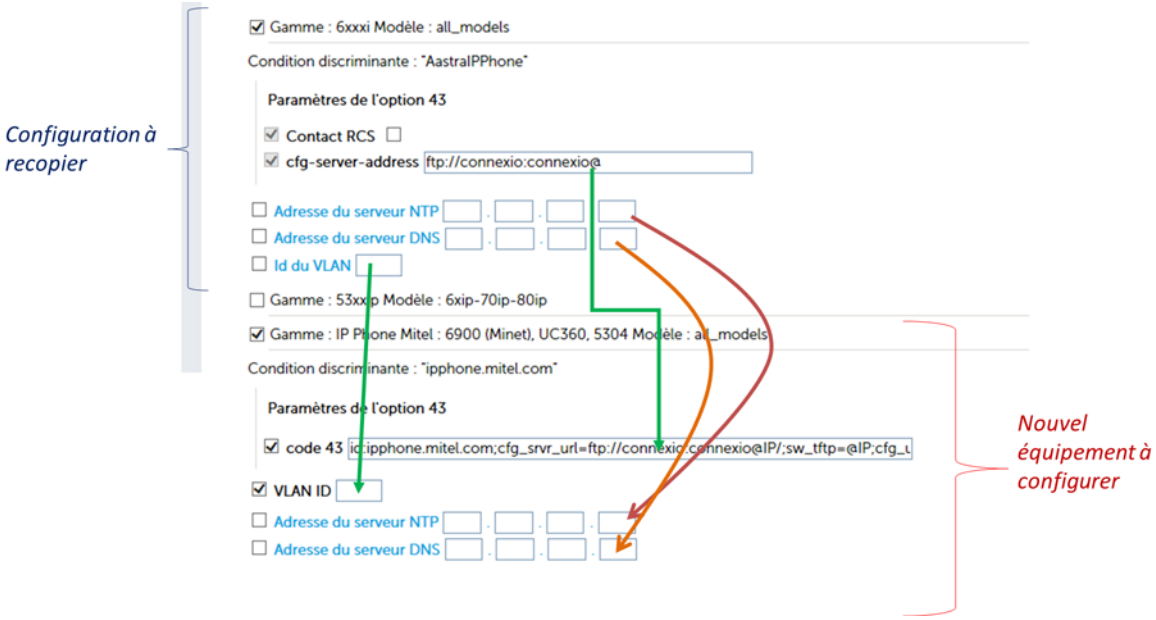

**Example of a configuration obtained through automatic upgrade**

For each subnet, if this latter is managing "**6xxxi / allmodels"**, the new device is also managed by this subnet, and the data specific to this device is initialised with that of "**6xxxi/allmodels**", more precisely:

- The "**cfg_srvr_url**" part of the character string which appears in the parameter "**code 43**" contains the value entered for the parameter "**cfg-server-address**" of the device "**6xxxi / allmodels**", the remaining part of the string is not modified.

```
id:ipphone.mitel.com;cfg_srvr_url=VALEUR_6xxxi;sw_tftp=@IP;cfg_uri=http://
@IPserver/path;call_srv=@IP;mode=sip;dscp=2;\0x000
```

- The parameter "**VLAN ID**" is the same as the parameter "**VLAN Id**" of "**6xxxi/allmodels**".
- The parameter "**NTP server address**" is identical to the parameter of the same name of the device
- "**6xxxi/allmodels**".Le paramètre « **Adresse du serveur DNS** » est identique au paramètre de même nom de l'équipement « **6xxxi/allmodels** »
- The parameter "**DNS server address**" is identical to the parameter of the same name of the device " **6xxxi/allmodels**"




**Initialising the parameters in automatic mode**

The DHCP server is automatically restarted to take this new configuration into account.

## 9.14 "6XXXI/ALL_MODELS OR SPECIFIC MODEL" AND "MIVOICE CONFERENCE UNIT" SELECTED

### 9.14.1 DESCRIPTION

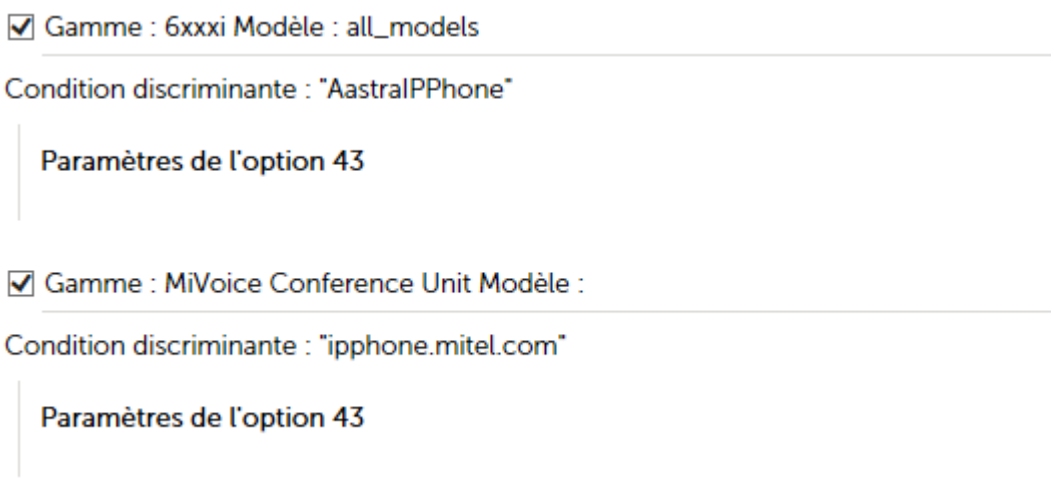
Below is a description of how to add the DHCP parameters used to manage terminals 6900, in a configuration already managing terminals 6xxxi and some UC360 devices (described in the template file *templateUC360.xml*), assuming that these new devices are only to be added to the subnets dedicated to terminals 6xxxi and/or MiVoice Conference Units..

### 9.14.2 PROCEDURE

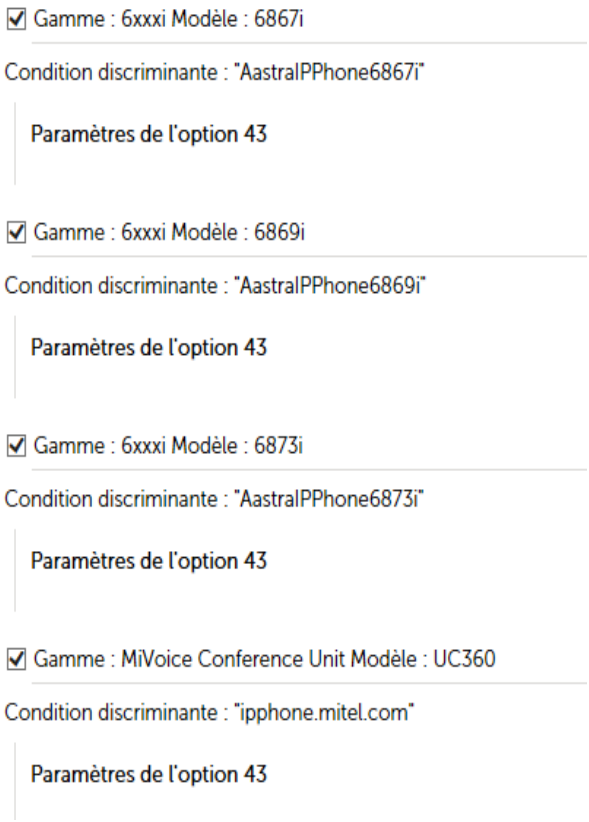
Via Web Admin, enter the integrated DHCP server administration. Select "**DHCP – Management**".

On the "Edit gobal parameters edition" screen, the following options must already be selected:

- "Range: 6xxxi Model: all_models"
- or "Range: 6xxxi Specific model"
- and "Range: MiVoice Conference Unit Model: ":




**Example with global management of terminals 6xxxi**




**Example with management of only certain 6xxxi models only**

Tick the option:

- "Range: Mitel IP Phone: 6900 (Minet), UC360, 5304 Model: all_models"

*Selecting the new device*




Editer **chaque sous-réseau** défini et si vous souhaitez qu'il gère cet équipement :

Edit **each subnet** defined and if you want it to manage this device:

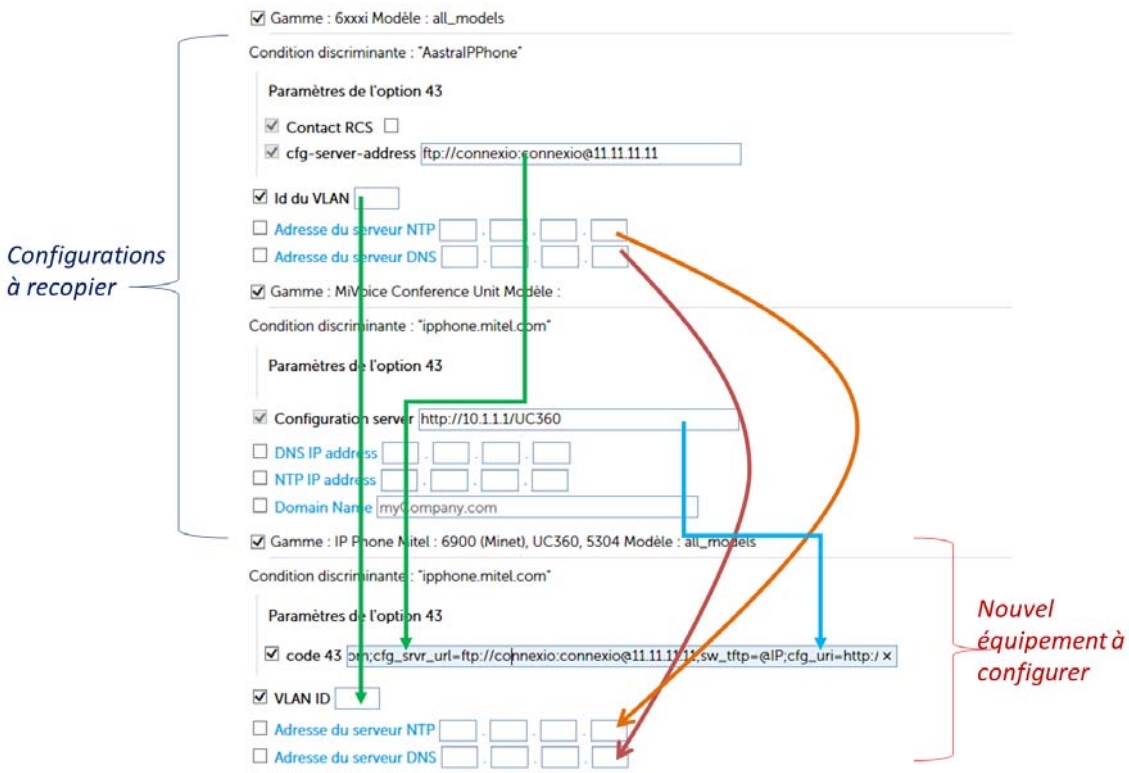
Tick "**Mitel IP Phone: 6900 (Minet), UC360, 5304 / all_models**" then initialise the values for this device from those entered for "**MiVoice Conference Unit**" and "**6xxxi/allmodels**" as follows:

- The "***cfg_srvr_url***" part of the character string which appears in the parameter "***code 43***" must contain the value entered for the parameter "***cfg-server-address***" of
- "**6xxxi**", and the "***cfg_uri***" part of this same string must contain the value entered for the "***Configuration server***" parameter of "**MiVoice Conference Unit** ", the remaining string should not be modified.

```
id:ipphone.mitel.com;cfg_srvr_url=VALEUR_6xxxi;sw_tftp=@IP;cfg_uri=VALEUR_UC360;call_srv=@IP;mode=sip;dscp=2;\0x000
```

- The parameter "**VLAN ID**" must be identical to the parameter "**VLAN** Id" of terminal "**6xxxi**".
- The parameter "**NTP server address**" must be identical to the parameter of the same name of terminal "**6xxxi**".

- The parameter "**DNS server address**" must be identical to the parameter of the same name of terminal "6xxxi"




**Summary of the modifications**

Validate the subnet modifications then go to the next subnet.

After all the subnets have been modified, return to the "Edit global parameters" screen, unselect "**MiVoice Conference Unit**".

Then generate the configuration, possibly with immediate effect.

Go to Menu "**Manage templates**" and delete the template "*templateUC360.xml*" which is no longer required.

## 9.15 "6XXXI/ALL_MODELS OR SPECIFIC MODEL" AND "UC360_5304" SELECTED

### 9.15.1 DESCRIPTION

Below is a description of how to add the DHCP parameters used to manage terminals 6900, in a configuration already managing terminals 6xxxi and some MiVoice Conference Units and MiVoice 5304 IP Phones (described in the template file *templateIpPhoneMitel.xml*), assuming that these new devices are only to be added to the subnets dedicated to terminals 6xxxi and/or MiVoice Conference Units and MiVoice 5304 IP Phones.

### 9.15.2 PROCDURE

Via Web Admin, enter the integrated DHCP server administration. Select "**DHCP – Management**".

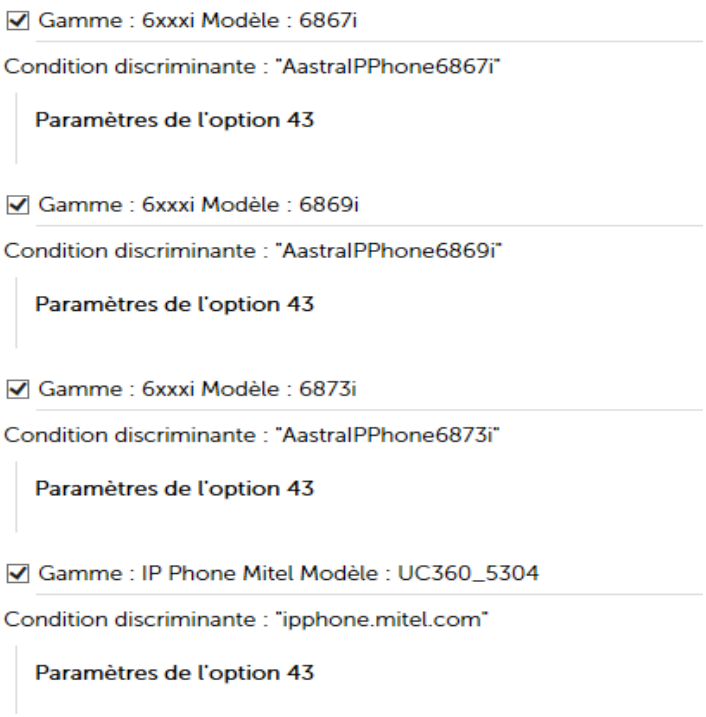
On the "Edit global parameters" screen, the following options must already be selected:

- "Range: 6xxxi Model: all_models"
- or "Range: 6xxxi Model: specific model"

"Range: Mitel IP Phone Model: UC360_5304". ».




**Example with global management of terminals 6xxxi**




**Example with management of only certain 6xxxi models only**

Tick the option:

- "Range: Mitel IP Phone: 6900 (Minet), UC360, 5304 Model: all_models"

*Selecting the new device*




For each subnet, and if you want it to manage this device:

Tick "**Mitel IP Phone: 6900 (Minet), UC360, 5304 / all_models** " then initialise the values for this device from those entered for the two devices, as follows:

- The "***sw_tftp***", "***cfg_uri***" and "***call_srv***" parts of the character string, which appear in the parameter "***code 43***", must contain the values entered in the character string for the "***code 43***" of the device "**UC360_5304**", the "***cfg_srvr_url*** " part must contain the value entered for the parameter "***cfg-server-address***" of terminal "**6xxxi**", the remaining part of the string is not modified.

```
id:ipphone.mitel.com;cfg_srvr_url=VALEUR_6xxxi;sw_tftp=VALEUR_UC360_5304;cfg_uri=VALEUR_UC360_5304;call_srv=VALEUR_UC360_5304;mode=sip;dscp=2;\0x000
```

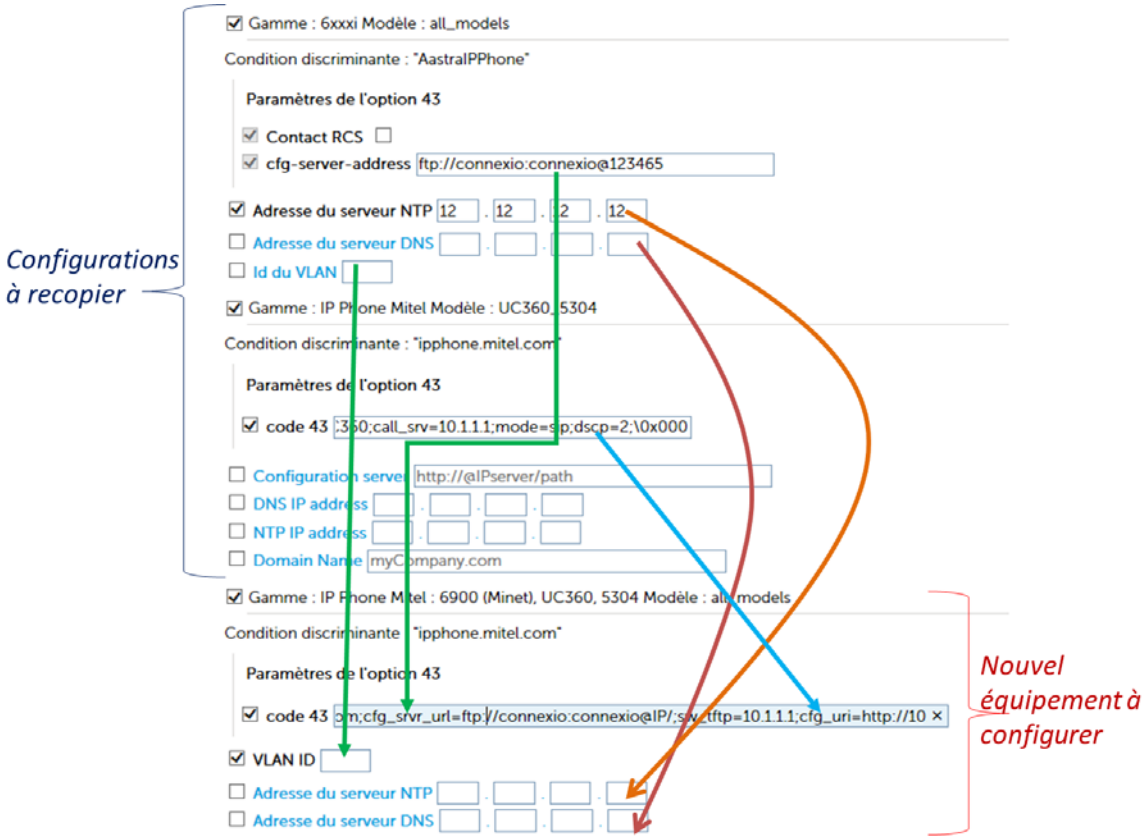
- The parameter "***VLAN ID***" must be identical to the parameter "***VLAN*** Id" of terminal "**6xxxi**".

**Note**: for the VLAN, if only terminals 5304 and 6900 are managed on this subnet, the parameter "**vlan**" can be added to the character string of the parameter "**code 43**" instead of using the parameter "**VLAN ID**".

Example:

```
id:ipphone.mitel.com;cfg_srvr_url=VALEUR_6xxxi;sw_tftp=VALEUR_UC360_5304
;cfg_uri=VALEUR_UC360_5304;call_srv=VALEUR_UC360_5304;mode=sip;dscp=2;vlan=VALEUR_6xxxi_idvlan;\0x000
```

The parameter "**NTP server address**" must be identical to the parameter of the same name of terminal "**6xxxi**".




**Summary of the modifications**

VValidate the subnet modifications then go to the next subnet.

After all the subnets have been modified, return to the "Edit global parameters" screen, unselect "**Range**". **Mitel IP Phone Model: UC360_5304**"

Then generate the configuration, possibly with immediate effect.

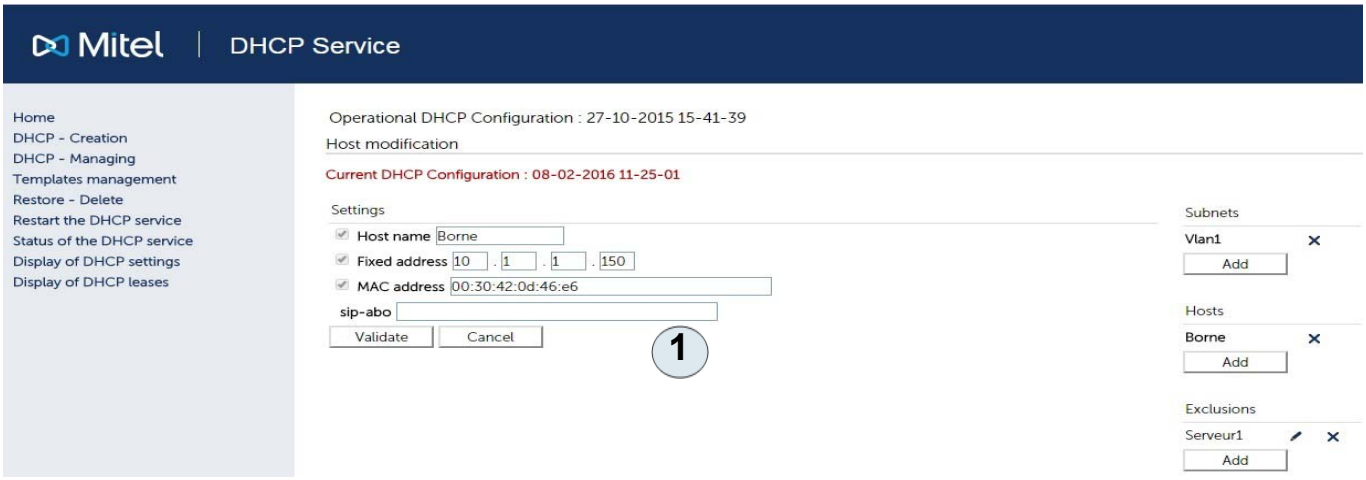
Go to Menu"Manage**templates** »and delete the template "*templateIpPhoneMitel.xml*" which is no longer required.

## 9.16 CONFIGURING THE PARAMETERS OF A SUBNET HOST

A host must be created for each IP DECT base station and each wifi terminal 312i available on the subnet in question.

- WIFI terminal 312i version 1.09 or later
- IP DECT base station version 1.04.

Click **Add** (**Hosts** column) to create a host on the subnet in question. This button is accessible on the configuration page of the subnet in question and also on the configuration page of a host and an exclusion.




1 The **sip-abo** field only appears if the wifi 312i range has been selected in the configuration parameters of the subnet in question.

Enter the following parameters:

- Host name
- Fixed address: IP address reserved for the host
- MAC address: Host MAC address.

**ATTENTION : Use the character : as separator.**

- sip-abo: obligatory parameter for a terminal 312i defining its SIP User ID (SIP subscription number defined in the Mitel 5000 Gateways system associated with terminal 312i). For a subnet with IP DECT base stations and terminals 312i, do not enter this parameter while creating hosts for IP DECT base stations.

**ATTENTION : Each host inherits some specific and standard configuration parameters defined for its range of terminals on the subnet in question.**

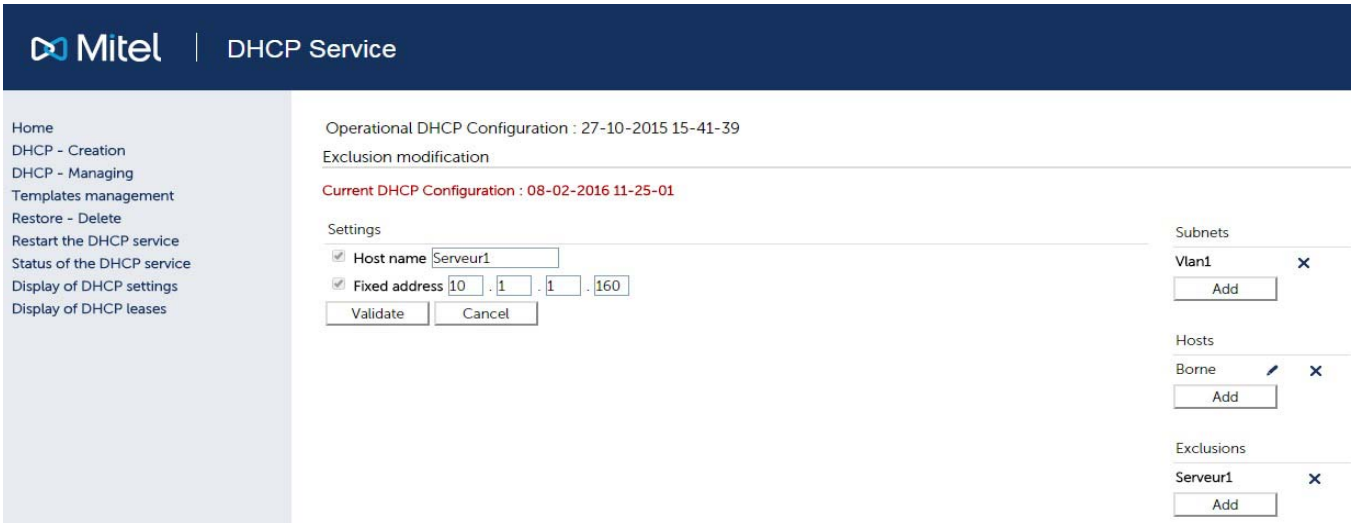
**ATTENTION : The IP address reserved for a host is automatically removed from the IP address range of the subnet in question. After a host is deleted, the reserved IP address is again available and reassigned to the IP address range of the subnet in question.**

Confirm the current configuration by clicking the **Validate** button.

## 9.17 CONFIGURING THE PARAMETERS OF A SUBNET EXCLUSION

It may be necessary to create an exclusion if a network device other than the terminals managed by the DHCP server is available on the subnet in question with a fixed IP address included in the IP address range defined for this subnet.

Click **Add** (**Exclusions** column) to create an exclusion on the subnet in question. This button is accessible on the configuration page of the subnet in question and also on the configuration page of a host and an exclusion.




Enter the following parameters:

- Host name
- Fixed address: Excluded IP address

**ATTENTION : The IP address associated with an exclusion is automatically removed from the IP address range of the subnet in question. After an exclusion is deleted, the excluded IP address is again available and reassigned to the IP address range of the subnet in question.**

Confirm the current configuration by clicking the **Validate** button.

# 9.18 TEMPLATES MANAGEMENT

As of R6.2, the integrated DHCP server allows new devices to be managed through template import.

This template file is an XML file containing the description of the new device, i.e. the description of its Vendor Class used to characterise this device and the parameters required for this device.

Several Vendor Classes can be defined for the same device.

By default, some template files are available in the integrated DHCP server configuration:

- TA7102i.xml
- UC360.xml

These two templates are available after R62.1 is newly installed or after an upgrade to R6.2.

## 9.18.1 ADDING A NEW TEMPLATE

This procedure describes the actions to take in order to add a new template and include it in the integrated server configuration.

### *9.18.1.1 Adding a new template*

- Click the **DHCP Service** menu.
- Click the **Template management** menu.
- Click **Choose a file,** then browse through the folders on the hard disk to select the XML file which describes the new template to install.
- Click **[Add]**.



**Note : While adding a new template, some consistency checks are made before importing it, to ensure that:**

- **A template with the same name is not already installed,**
- **The syntax is correct,**
- **The template describes the device correctly,**
- **The device described in the template is not already open in another template file.**



**ATTENTION : The creation of a new template file is managed by the development/Support teams, which are also in charge of updating the existing template files.**

**These template files are available on the Support Extranet.**

### *9.18.1.2 Configuring and taking the new template into account*

- Click the **DHCP Service** menu.
- Click the **DHCP - Operation** menu.
- In the global parameters, tick the new device associated with the new template.
- Click the  icon to modify the subnet in question. The subnet parameters definition page opens.
- In the subnet concerned, tick the new device associated with the new template to be taken into account in the integrated DHCP server configuration.

- Modify the specific parameters of the new device with the new values you want.
- Save the new configuration by clicking **Validate**.



**Note : To avoid taking account of the modifications made, click Cancel.**

- From the global parameters edition page, click **Generate**.
- After the file dhcpd.conf is generated with the new configuration, an option is proposed allowing the new configuration of the integrated DHCP server to be taken into account immediately or later.
  - Click **Yes** to immediately take into account the new configuration of the integrated DHCP server, by immediately restarting the DHCP service. An information message then gives the status of the DHCP service: the DHCP service is started.
  - Click **No** so the new integrated DHCP server configuration is not taken into account. In that case, it will be necessary to use Menu **Restart DHCP service** to take into account, at the required moment, the new configuration of the integrated DHCP server, by restarting the DHCP service.



**ATTENTION : The Template Management menu is used to list the installed template files and know the versions associated with these templates.**

**If a new version of template file must be installed, the previoud version of this template file must be deleted before installing the new version.**

## 9.18.2 DELETING AN EXISTING TEMPLATE

This procedure describes the actions to take in order to delete an existing template and take its deletion into account in the integrated DHCP server configuration.

### *9.18.2.1 Deleting an existing template*

- Click the **DHCP Service** menu.
- Click the **Template management** menu.
- Select by name the template file to delete then click **Delete.**
- Click **Yes** to confirm the template file deletion.



**ATTENTION : The template file will not appear any longer in the integrated DHCP server configuration menus, but a generation is necessary so this device is no longer functionally managed by the integrated DHCP server.**

### *9.18.2.2 Taking into account the template file deletion*

- From the global parameters edition page, click **Generate**.
- After the file dhcpd.conf is generated with the new configuration, an option is proposed allowing the new configuration of the integrated DHCP server to be taken into account immediately or later.
  - Click **Yes** to immediately take into account the new configuration of the integrated DHCP server, by immediately restarting the DHCP service. An information message then gives the status of the DHCP service: the DHCP service is started.

- Click **No** so the new integrated DHCP server configuration is not taken into account. In that case, it will be necessary to use Menu **Restart DHCP service** to take into account, at the required moment, the new configuration of the integrated DHCP server, by restarting the DHCP service.

## 9.19 GENERATING THE CONFIGURATION FILE USED BY THE INTEGRATED DHCP SERVER

When all the subnet parameters are defined, it is mandatory to generate the file dhcpd.conf . This is the configuration file used by the integrated DHCP server.

To generate the file dhcpd.conf:

- From the global parameters edition page, click **Generate**.
- After the file  dhcpd.conf is generated with the new configuration, an option is proposed allowing the new configuration of the integrated DHCP server to be taken into account immediately or later.
    - Click **Yes** to immediately take into account the new configuration of the integrated DHCP server, by immediately restarting the DHCP service. An information message then gives the status of the DHCP service: the DHCP service is started.
    - Click **No** so the new integrated DHCP server configuration is not taken into account. In that case, it will be necessary to use Menu **Restart DHCP service** to take into account, at the required moment, the new configuration of the integrated DHCP server, by restarting the DHCP service.

## 9.20 MODIFYING THE PARAMETERS OF A DHCP CONFIGURATION

From the DHCP service home page, click the **DHCP - Operation** menu.

The global parameters are displayed, as well as the defined subnet(s).

- Click the icon to modify the subnet in question. The subnet parameters definition page opens.
- Modify the network parameters with new values you want.
- Modify, if necessary, the parameters associated with hosts and/or exclusions by clicking the icon concerned.

**Note : The icon is used to delete a subnet, host or exclusion.**

- Save the new configuration by clicking **Validate**.

**Note : To avoid taking account of the modifications made, click Cancel.**

- From the global parameters edition page, click **Generate**.
- After the file dhcpd.conf is generated with the new configuration, an option is proposed allowing the new configuration of the integrated DHCP server to be taken into account immediately or later.
  - Click **Yes** to immediately take into account the new configuration of the integrated DHCP server, by immediately restarting the DHCP service. An information message then gives the status of the DHCP service: the DHCP service is started.
  - Click **No** so the new integrated DHCP server configuration is not taken into account. In that case, it will be necessary to use Menu **Restart DHCP service** to take into account, at the required moment, the new configuration of the integrated DHCP server, by restarting the DHCP service.

## 9.21 RESTORING AND DELETING AN ARCHIVE

An archive is created automatically each time the **Generate** button is clicked.

To view the available archives, click the **Restore - Suppress** menu from the **DHCP Service** home page.

Each archive is time-stamped, with a version. The archives are also arranged in chronological order.

To delete an archive:

- Select the archive and click **Delete**.
- Confirm the deletion by clicking **Confirm**.

To restore an archive:

- Select the archive and click **Restore**.
- Confirm the restore operation by clicking **Confirm**.



**Note : An archive contains the entire configuration data for the integrated DHCP server, including the installed and configured template files.**

For the DHCP server to take account of this archive:

- From the global parameters edition page, click **Generate**.
- After the file dhcpd.conf is generated with the new configuration, an option is proposed allowing the new configuration of the integrated DHCP server to be taken into account immediately or later.
    - Click **Yes** to immediately take into account the new configuration of the integrated DHCP server, by immediately restarting the DHCP service. An information message then gives the status of the DHCP service: the DHCP service is started.
    - Click **No** so the new integrated DHCP server configuration is not taken into account. In that case, it will be necessary to use Menu **Restart DHCP service** to take into account, at the required moment, the new configuration of the integrated DHCP server, by restarting the DHCP service.

## 9.22 VIEWING THE DHCP SERVER CONFIGURATION

Two pieces of information are used to know the DHCP server configuration status at any time:

- **File definition in progress,**
- **File operational,**

The **operational file** corresponds to the configuration with which the DHCP server started the last time. This information is updated each time the DHCP server restarts (Click the menu **Restart DHCP service or** answer **Yes** after the last generation via the **Generate** button).

**File definition in progress** corresponds to the last configuration displayed in the DHCP service MMI. This information is updated each time a modification is made in the DHCP service MMI (click the **Validate** button or answer No after the last generation via the **Generate** button).

In nominal operation mode, the information must be identical (to within one second). This makes it possible to know that the information displayed in the DHCP service MMI corresponds to the information currently used by the DHCP server.

## 9.23 DHCP SERVICE STATUS:

The **DHCP service status** menu is used to display the status of the DHCP service:

- The DHCP service is started.
- The DHCP service is stopped.

## 9.24 VIEW DHCP LEASES

The menu **View dhcp leases** is used to display the content of the file dhcpd.leases.

## 9.25 CONFIGURATION WITH TWO SUBNETS IN SHARED NETWORK MODE.

If two subnets are managed by the integrated DHCP server and the integrated DHCP server belongs to any of the two subnets, a special configuration mode must be defined for the subnet concerned:

- shared-network configuration

To specify that the subnet is configured in shared-network mode, proceed as follows:

- From the **DHCP service** home page, click the **DHCP - Operation** menu.
- Click the  icon to modify the subnet in question. The subnet parameters definition page opens.
- In the configuration window of the subnet concerned, tick the field **Gateway shares this subnet.**
- Save the new configuration by clicking **Validate**.
- From the global parameters edition page, click **Generate**.
- After the file dhcpd.conf is generated with the new configuration, an option is proposed allowing the new configuration of the integrated DHCP server to be taken into account immediately or later.
    - Click **Yes** to immediately take into account the new configuration of the integrated DHCP server, by immediately restarting the DHCP service. An information message then gives the status of the DHCP service: the DHCP service is started.
    - Click **No** so the new integrated DHCP server configuration is not taken into account. In that case, it will be necessary to use Menu **Restart DHCP service** to take into account, at the required moment, the new configuration of the integrated DHCP server, by restarting the DHCP service.

## 9.26 MANAGING INTEGRATED DHCP SERVER DATA WHILE BACKING UP DATA FROM MIVOICE 5000

During MiVoice 5000 data backup, the following integrated DHCP server data are backed up:

- The configuration of the integrated DHCP server,
- The configuration data archives of the integrated DHCP server,
- The installed templates.

After a MiVoice 5000 data restore, all the previously backed up data are restored. For these data to be taken into account by the integrated DHCP server, the configuration file used by the integrated DHCP server must be generated (see Chapter 9.19).

## 9.27 MANAGING THE INTEGRATED DHCP SERVER DATA WHILE UPGRADING MIVOICE 5000

During MiVoice 5000 upgrade, the following integrated DHCP server data are kept:

- The configuration of the integrated DHCP server,
- The configuration data archives of the integrated DHCP server,
- The installed templates.

If during a MiVoice 5000 upgrade, a template file changes (new parameter), taking this change into account requires generating the configuration file used by the integrated DHCP server (see Chapter 9.19).

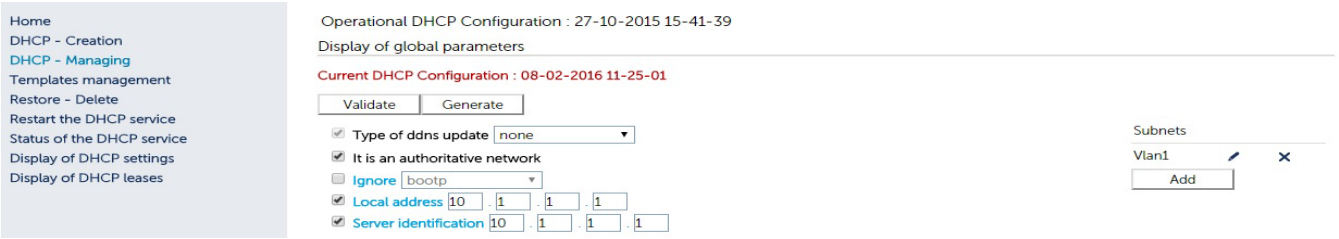
# 9.28 REDUNDANT INTEGRATED DHCP SERVER ON A REDUNDANT MIVOICE 5000 SERVER

**ATTENTION : As of R6.2, in a redundant MiVoice 5000 Server configuration, the DHCP server integrated into MiVoice 5000 Server systems is available. In this case, the virtual IP address can be configured in the integrated DHCP server.**

As of R6.2, the **CTRL I** menu of a redundant MiVoice 5000 Server proposes to install or not to install the DHCP service.

If the DHCP service is installed, automatically the following global parameters are entered with the virtual IP address of the redundant MiVoice 5000 Server:

- Local address
- Server ID




The integrated DHCP service is automatically started on the active MiVoice 5000 Server and stopped on the inactive MiVoice 5000 Server.

The integrated DHCP server configuration is automatically duplicated from the active MiVoice 5000 Server machine to the inactive MiVoice 5000 Server.

When a redundant MiVoice 5000 Server is being upgraded to R6.2, and the integrated DHCP service installed, taking into account the two new configuration parameters described above requires generating the configuration file used by the integrated DHCP server (see Chapter 9.19).

The configuration data of an integrated redundant MiVoice 5000 Server is taken into account during redundant MiVoice 5000 Server data backup and restore procedures as well as during redundant MiVoice 5000 Server upgrade.

# 10 CONFIGURING AN EXTERNAL DHCP SERVER

## 10.1 CONFIGURING THE EXTERNAL DHCP SERVER FOR MITEL 6000 SIP PHONES

### 10.1.1 STANDARD DHCP SETTINGS OR OPTIONS MANAGED BY MITEL 6000 SIP PHONES

Mitel 6000 SIP Phones integrate a DHCP client.
The table below describes the standard options managed by Mitel 6000 SIP Phones.

| STANDARD DHCP SETTINGS OR OPTION | NOTE: |
|---|---|
| IP address and subnet mask (option 1) | parameter required in option 55 |
| Gateway IP address (option 3) | parameter required in option 55 |
| DNS server IP address (option 6) | parameter required in option 55 |
| NTP server IP address (option 42) | parameter required in option 55 |
| Vendor-specific option (option 43) | parameter required in option 55 |
| Vendor-class-specific information (option 60) | * See the table below. |
| FTP server IP address (option 66) | ftp://connexio:connexio@'FTP server IP address' |
| VLAN ID (option 132)** | parameter required in option 55 |

* Name of the Vendor Classes used by Mitel 6000 SIP Phones according to terminal model:

| TERMINAL MODEL | VENDOR CLASS |
|---|---|
| A6751SIPi | AastraIPPhone51i |
| 6753 SIP | AastraIPPhone53i |
| 6755 SIP | AastraIPPhone55i |
| 6757 SIP | AastraIPPhone57i |
| 6730 SIP | AastraPPhone6730i |
| 6731 SIP | AastraIPPhone6731i |
| 6735 SIP | AastraPPhone6735i |
| 6737 SIP | AastraIPPhone6737i |
| 6739 SIP | AastraPPhone6739i |
| 6863 SIP | AastraIPPhone6863i |
| 6865 SIP | AastraIPPhone6865i |
| 6867 SIP | AastraIPPhone6867i |
| 6869 SIP | AastraIPPhone6869i |
| 6873 SIP | AastraIPPhone6873i |
| BluStar 8000i | AastraBluStar8000i |

**ATTENTION : Negotiating Option 132 option through DHCP option requires setting the DHCP option 132 parameter vlan id enabled to 1 in the global or specific configuration file used by Mitel 6000 SIP phone (aastra.cfg ou <mac>.cfg).**

The order of priority for the VLAN ID to be taken into account by Mitel 6000 SIP Phone is as follows:

- 1. VLAN ID negotiated via LLDP (highest priority)
- 2. VLAN ID negotiated via DHCP (option 43 with a priority above that of option 132)
- 3. VLAN ID configured via the terminal's WEB interface
- 4. VLAN ID configured via aastra.cfg or <mac>.cfg

### 10.1.2 SPECIFIC DHCP SETTINGS MANAGED BY MITEL 6000 SIP PHONES VIA OPTION 43

Mitel 6000 SIP Phone send Option 60 of the DHCP protocol (vendor class identifier) in the DHCP request (discover/request) to identify themselves. Moreover, Mitel 6000 SIP Phones prompt the DHCP server for vendor specific information, by specifying option 43 in their list of requests for parameters associated with option 55. If the DHCP server is configured to react to the vendor specific identifier, it will add option 43 (vendor specific information) to these replies.

The table below describes all the parameters that can be negotiated via Option 43 with Mitel 6000 SIP Phones:

| SPECIFIC PARAMETERS (OPTION 43) | CODE | HEX. VALUE CODE | LENGTH/ TYPE | NOTE: |
|---|---|---|---|---|
| cfg-server-address | 10/02 | 10/02 | String | FTP server IP address.<br>example: ftp://connexio:connexio@192.168.245.1 |
| cfg-contact-rcs | 10/03 | 10/03 | Booleen | RCS deactivation: set the value to **false** |
| VLAN_ENABLED | 10/08 | 10/08 | 16 bytes/ text | Value in Hexa:<br>41 61 73 74 72 61 20 54 65 6c 65 63 6f 6d 20 20<br>(corresponds to "Aastra Telecom" followed by 2 spaces) |
| VLAN_ID | 10/09 | 10/09 | 4 bytes/ integer | Specifies the VLAN ID used by the terminal's VLAN port.<br>(example: 00 00 00 64 for vlan 100) |

**ATTENTION : Set the parameter cfg-contact-rcs to false.**
**Codes 08 and 09 must be negotiated together.**

## 10.1.3 CONFIGURING A DHCP SERVER ON A WINDOWS 2000/2003 PLATFORM FOR MITEL 6000 SIP PHONES

### *10.1.3.1 Configuring standard network parameters from the DHCP server*

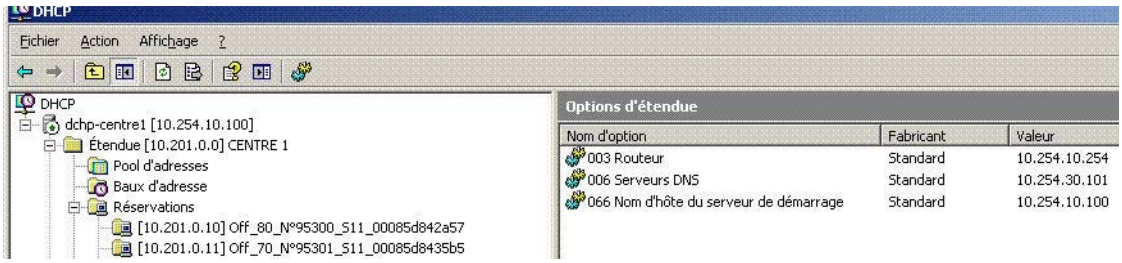
By default, the terminal is set to DHCP enabled and uses the TFTP.

Principle

The first time it is connected, the terminal makes a DHCP request to all the DATA defined on the DHCP server. This DATA on the DHCP server must contain the following options:

- Standard option 03: Router (gateway) IP address
- Standard Option 66: FTP, login/password and FTP server IP address

  or
- Specific Option 43, code 02: FTP, login/password and FTP server IP address




**Note : As of version 2.1 of Mitel 6000 SIP Phones, Option 43, code 2 allows you to negotiate with the DHCP server the FTP server address and its associated login and password.**

**ATTENTION : For an existing installation in which Mitel 6000 SIP Phone with versions below 2.1 are already in service and rely on a TFTP server for their update, it is important to update the terminal via the TFTP server to version 2.1 then modify the DHCP server configuration to negotiate via Option 43 the FTP server address with its associated login and password.**

The IP address range associated with the DATA range must be enough to provide a temporary IP address to each Mitel 6000 SIP Phone when it is first installed on the LAN.

During this first transaction with the DHCP server in the DATA VLAN, the DHCP server assigns to each terminal:

- A temporary IP address
- Its temporary subnet mask
- The DATA subnet gateway (router) IP address
- The FTP server IP address with its login and password

This first DHCP transaction in the DATA range enables Mitel 6000 SIP Phone to update its firmware with the current version compatible with the MiVoice 5000 solution and recover all the network parameters necessary to work correctly via the global and specific configuration files. These files are available in the FTP server storage area used to deploy Mitel 6000 SIP Phone.

The global and specific configuration files enable the terminal, among others, to recover its VLAN ID with its associated priority. After this modification, the terminal will restart to take into account these new network parameters, and the temporary IP address taken by the terminal will be released.

**ATTENTION : If necessary, the terminal VLAN may be configured through DHCP as of terminal release 3.3.1 (option 43 codes 07 and 08 or standard option 132)**
**Negotiating option 132 via DHCP requires setting the parameter dhcp option 132 vlan id enabled to 1 (aastra.cfg, <mac>.cfg).**

When Mitel 6000 SIP Phone is started for a second time, the terminal makes a second DHCP transaction by querying the Mitel 6000 SIP Phone TERMINAL range defined on the DHCP server. This Mitel 6000 SIP Phone TERMINAL range on the DHCP server must contain the following options:

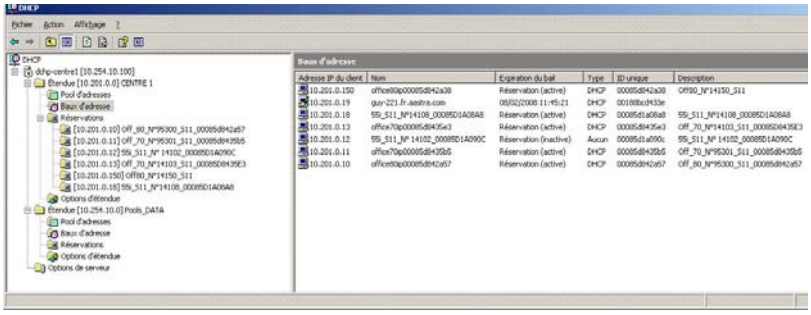
- Standard option 03: Router (gateway) IP address
- Standard Option 66: FTP, login/password and FTP server IP address

  or

- Specific Option 43, code 02: FTP, login/password and FTP server IP address.

**Note : As of version 2.1 of Mitel 6000 SIP Phones, specific Option 43 allows you to negotiate with the DHCP server the FTP server address and its associated login and password.**

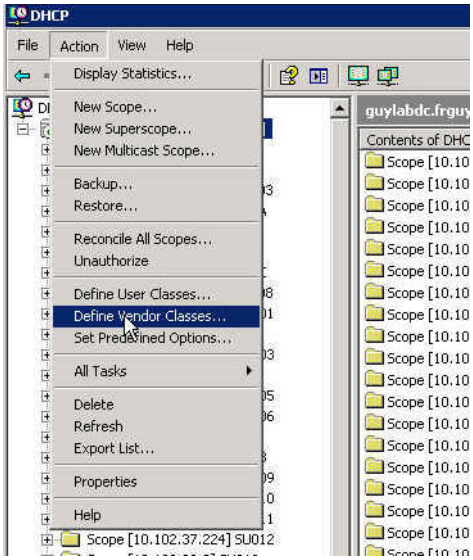
Standard option 66 or specific Option 43, Code 02 can be associated either with the full range or on terminal basis by creating IP address reservations from the MAC addresses of each Mitel 6000 SIP Phone. This reservation from MAC addresses may become obligatory if different terminal models are combined in the same range (the same subnet) and do not use the same FTP server.



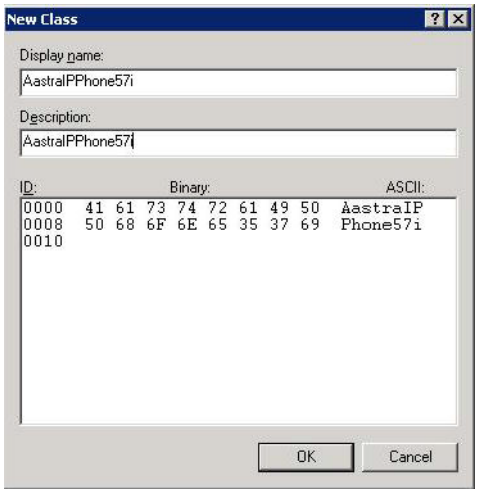
### *10.1.3.2 Configuring the vendor class and options associated with the DHCP server*

In the DHCP server management interface:

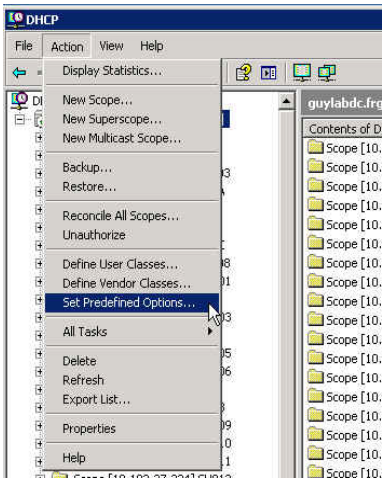
Select the column Action/Define Vendor Classes




In the following window, enter in the ASCII area the value corresponding to the identifier of the model of Mitel 6000 SIP Phone concerned.



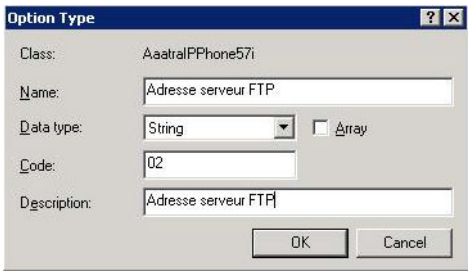
Then select the column Action/Set Predefined Options.



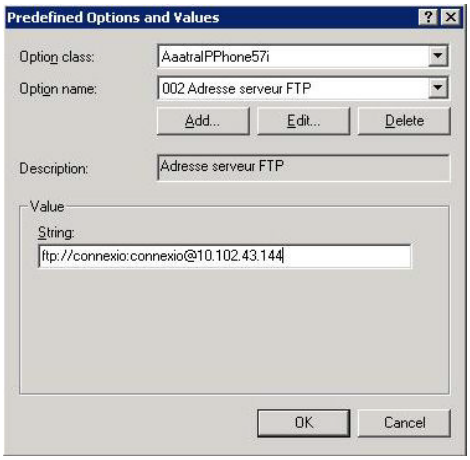

Select the vendor class “AastraIPPhone57i” in the “Option Class” field then click Add. Enter:

- The name of the option to be created: cfg-server
- Type of data: String
- The code associated with the option: 10/02
- The description associated with the option: FTP server address

The possible values of the first three fields are defined in the table in Chapter 10.1.2. Confirm the creation by pressing OK.

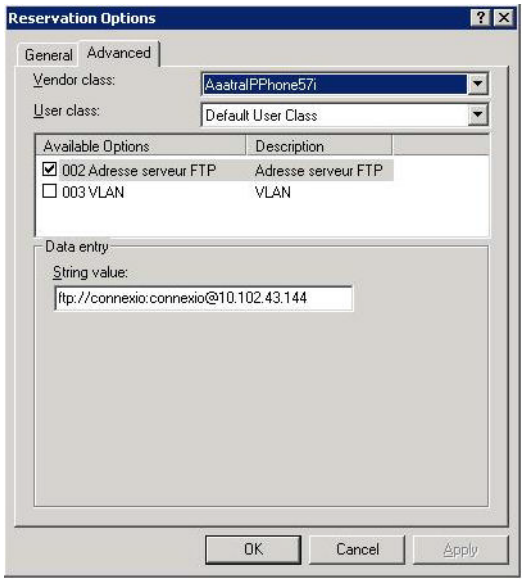


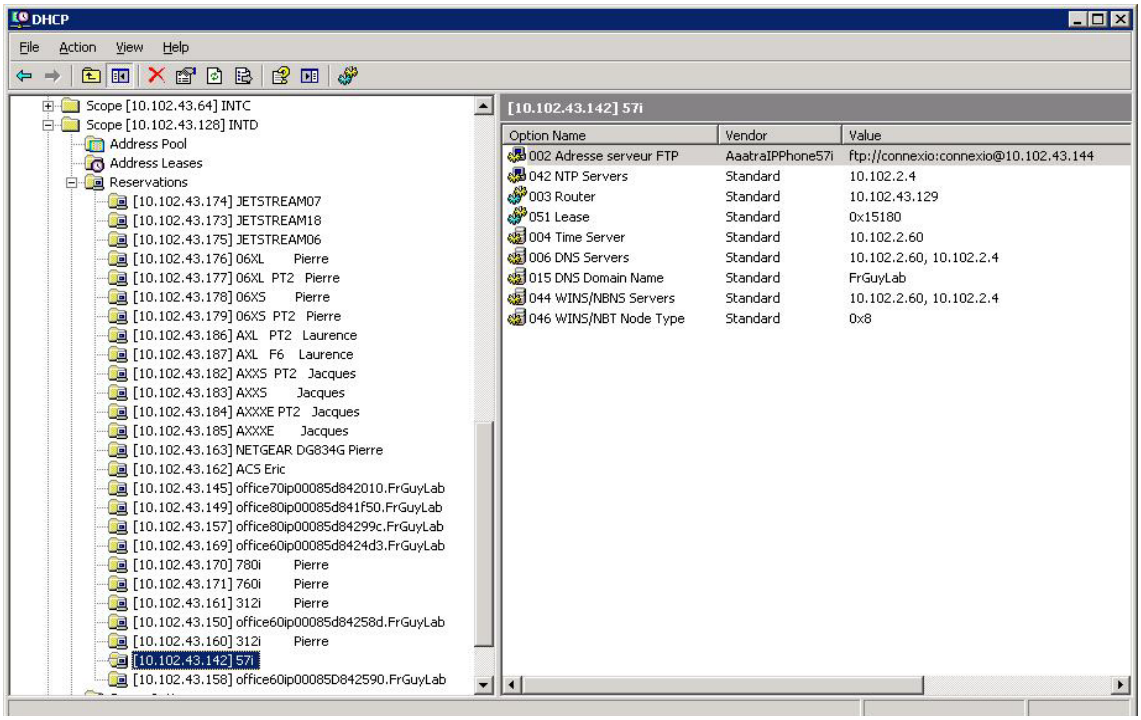

Return to the predefined options and values menu, then select the option just created to enter its default value  in the value field:




Configure using the same procedure in Option 3:

All the options defined for this class (vendor class) can be associated with all the DHCP server scopes (global options scope), with a specific scope (subnet options scope) or a specific terminal (configuration options of the reservation associated with the terminal) using the “Advanced” tab of the “Reservation Options” menu.



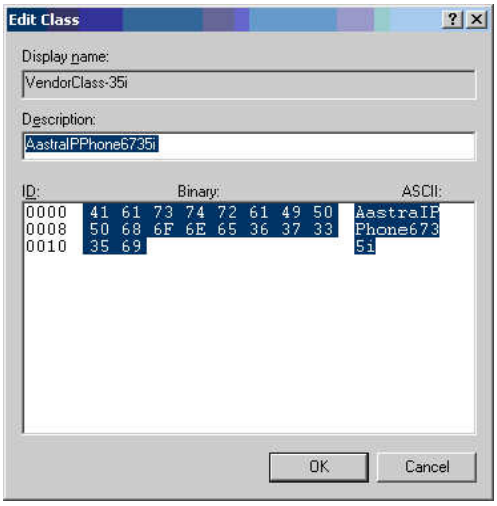



### *10.1.3.3 Example of external DHCP server configuration in Windows 2003 for terminals 6735 SIP, 6737 SIP, 6863 SIP, 6865 SIP, 6867 SIP, 6869 SIP and 6873 SIP*

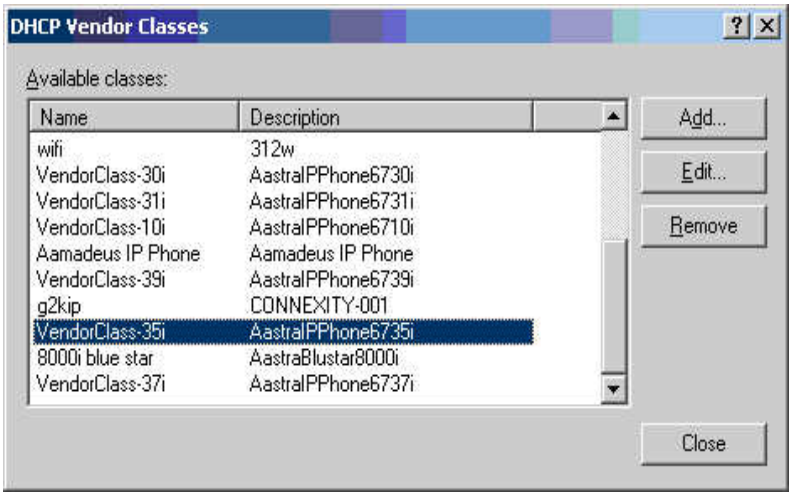
In this example, 6735 SIP, 6737 SIP, 6863 SIP, 6865 SIP, 6867 SIP, 6869 SIP and 6873 SIP phones negotiate VLAN ID 100 via option 43, and the RCS option is disabled.

**Note : The screenshots concern 6735 SIP phone.**

- Menu DHCP Server: definition of Vendor Classes
  - Add the Vendor classes of 6735 SIP, 6737 SIP, 6863 SIP, 6865 SIP, 6867 SIP, 6869 SIP and 6873 SIP phones.




- Example of DHCP Vendor Class list

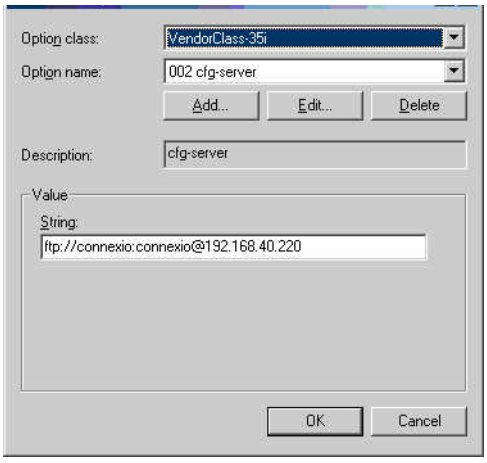


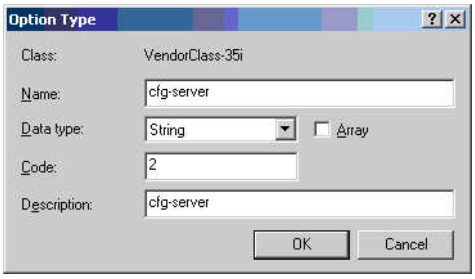
Menu DHCP Server: predefined options values

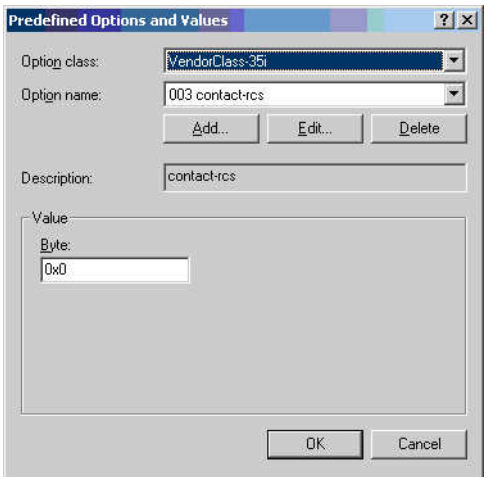
- Add the two options (code 2 and code 3) then configure the values associated with these two options for the Vendor Classes of 6735 SIP, 6737 SIP, 6863 SIP, 6865 SIP, 6867 SIP, 6869 SIP and 6873 SIP phones.

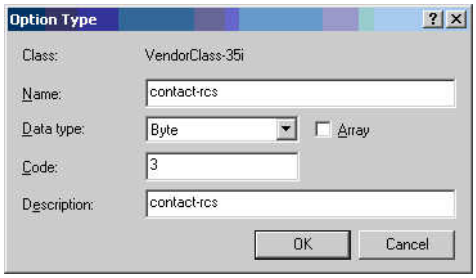
  Code 2 contains the IP address of the FTP server associated with the login/password used by default by 6735 SIP, 6737 SIP, 6863 SIP, 6865 SIP, 6867 SIP, 6869 SIP and 6873 SIP (connexio:connexio). Code 2 is of **String type.**

  Code 3 must be equal to 0 (RCS deactivation). Code 3 is of **Byte type.**



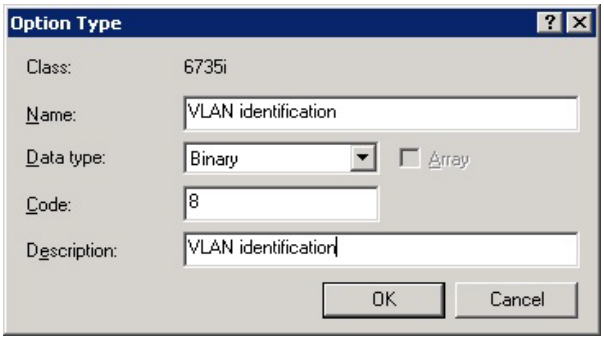
- Add the two options (code 8 and code  9) associated with the Vendor Classes of 6735 SIP, 6737 SIP, 6863 SIP, 6865 SIP, 6867 SIP, 6869 SIP and 6873 SIP phones.

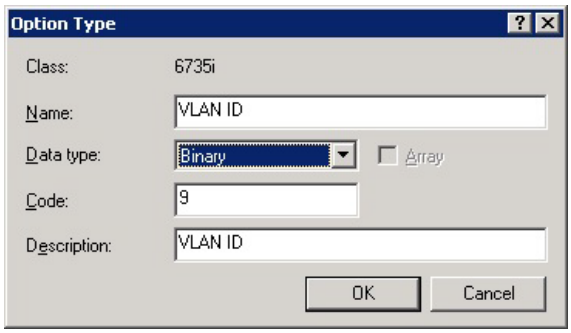
  Code 8 contains the identification of 6735 SIP, 6737 SIP, 6863 SIP, 6865 SIP, 6867 SIP, 6869 SIP and 6873 SIP phones which allows the use of the VLAN ID associated with code 9. Code 8 must contain the character string below: "Aastra{space}Telecom{space}{space}".

  The corresponding hexadecimal value is: 41617374726120546565636f6d2020
  Code 8 is of **Binary type.**

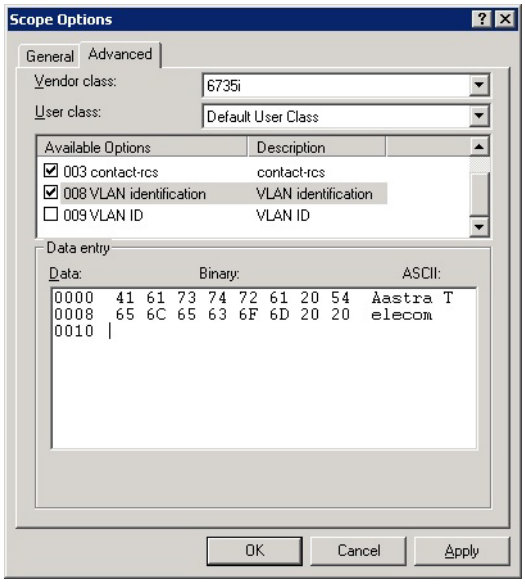
  Code 9 contains the VLAN ID of 6735 SIP, 6737 SIP, 6863 SIP, 6865 SIP, 6869 SIP and 6873 SIP phones. The first two bytes must be equal to 0, and the next two must contain the value of the VLAN ID.

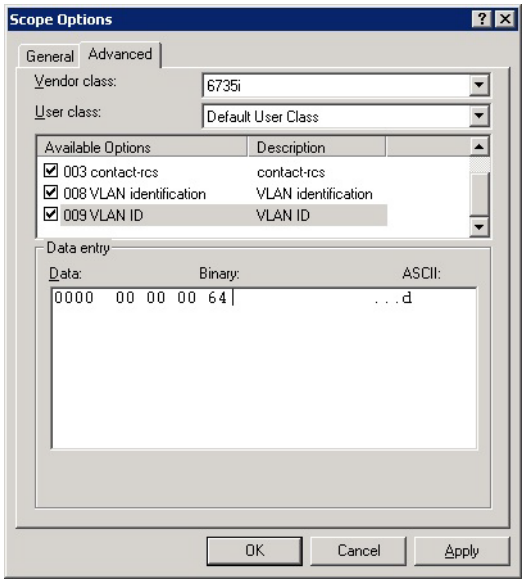
  A VLAN ID of 100 (in decimal) is coded as follows in hexadecimal: 00 00 00 64
  Code 9 is of **Binary type.**



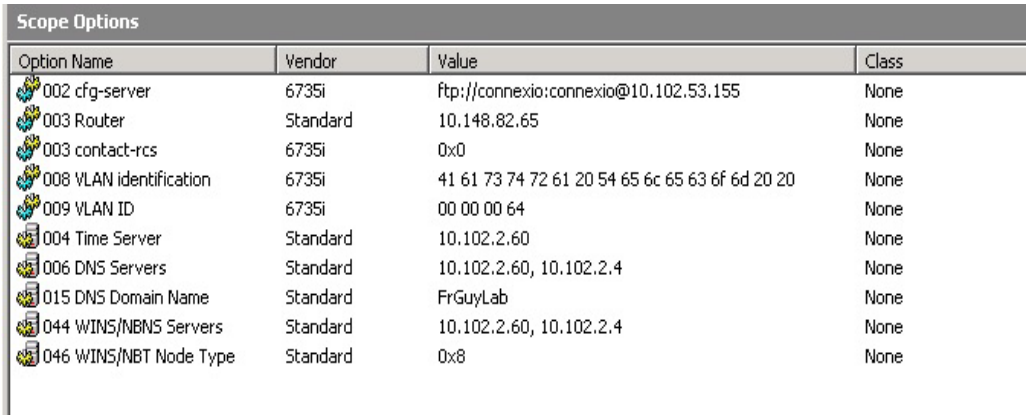



- Menu DHCP Server:  options scope of 6735 SIP, 6737 SIP, 6863 SIP, 6865 SIP, 6867 SIP, 6869 SIP and 6873 SIP phones:
  - In the advanced options of the range of 6735 SIP, 6737 SIP, 6863 SIP, 6865 SIP,  6867 SIP, 6869 SIP and 6873  SIP the parameters associated with the Vendor Classes of 6735 SIP, 6737 SIP, 6863 SIP, 6865 SIP, 6867 SIP, 6869 SIP and 6873 SIP phones (code 2, code 3, code 8 and code 9).
    - For each Vendor Class, tick options 2 and 3 (modify the default values if necessary).
    - For each Vendor class, tick option 8 and enter the 16 hexadecimal values.
    - For each Vendor class, tick option 9 and enter the 4 hexadecimal values.



Example of configuration of the options associated with the range of 6735 SIP, 6737 SIP, 6863 SIP, 6865 SIP, 6869 SIP and 6873 SIP phones



Scope Options

| Option Name | Vendor | Value | Class |
|---|---|---|---|
| 002 cfg-server | 6735i | ftp://connexio:connexio@10.102.53.155 | None |
| 003 Router | Standard | 10.148.82.65 | None |
| 003 contact-rcs | 6735i | 0x0 | None |
| 008 VLAN identification | 6735i | 41 61 73 74 72 61 20 54 65 6c 65 63 6f 6d 20 20 | None |
| 009 VLAN ID | 6735i | 00 00 00 64 | None |
| 004 Time Server | Standard | 10.102.2.60 | None |
| 006 DNS Servers | Standard | 10.102.2.60, 10.102.2.4 | None |
| 015 DNS Domain Name | Standard | FrGuyLab | None |
| 044 WINS/NBNS Servers | Standard | 10.102.2.60, 10.102.2.4 | None |
| 046 WINS/NBT Node Type | Standard | 0x8 | None |

### 10.1.4 CONFIGURING A DHCP SERVER ON A MIVOICE 5000 SERVER PLATFORM FOR MITEL 6000 SIP PHONES

The procedure for configuring a DHCP server on a LINUX platform is the same as the one described in Section 10.1.2.



**ATTENTION : UDP ports 67 and 68 must be open if the A5MiVoice 5000 Server firewall is enabled.**

In the example below, the DHCP server used is dhcpd. This package is not installed by default when RedHat Enterprise 5 is installed on the MiVoice 5000 Server platform. The installation of this package is described in the Appendix.

Proceed as follows:

**1. Configure the configuration file dhcpd.conf available in the directory /etc.**

The modifications consist in:

- Define all the vendor codes that can be used by Mitel 6000 SIP Phones.
- Define standard options 03, and 66 for the ToIP subnet.
- If necessary, define for each subnet concerned the MAC-address-based reservations for Mitel 6000 SIP Phones with the vendor options possibly used.



**ATTENTION : Set the value if the parameter cfg-contact-rcs to false for 6735 SIP, 6737 SIP, 6863 SIP, 6865 SIP, 6867 SIP, 6869 SIP and 6873 SIP.**

The file dhcpd.conf below is a non exhaustive example of a typical configuration including 6735 SIP, 6737 SIP, 6863 SIP, 6865 SIP, 6867 SIP, 6869 SIP and 6873 SIP phones.

- In this example, 6735 SIP, 6737 SIP, 6863 SIP, 6865 SIP, 6867 SIP, 6869 SIP and 6873 SIP phones negotiate VLAN ID 100 via option 43, and the RCS option is disabled.

```
ddns-update-style none;
authoritative;

# Declaration of the terminal structure 6735i
option space 6735i;
option 6735i.cfg-server-address code 2 = string;
option 6735i.cfg-contact-rcs code 03 = boolean;
option 6735i.ActivateVLANHeader code 08 = text;
option 6735i.VLAN-ID code 09 = unsigned integer 32;

# Declaration of the terminal structure 6737i
option space 6737i;
option 6737i.cfg-server-address code 2 = string;
option 6737i.cfg-contact-rcs code 03 = boolean;
option 6737i.ActivateVLANHeader code 08 = text;
option 6737i.VLAN-ID code 09 = unsigned integer 32;

# Declaration of the terminal structure 6863i
option space 6863i;
option 6863 i.cfg-server-address code 2 = string;
option 6863i.cfg-contact-rcs code 03 = boolean;
option 6863i.ActivateVLANHeader code 08 = text;
option 6863i.VLAN-ID code 09 = unsigned integer 32;

# Declaration of the terminal structure 6865i
option space 6865i;
```

```
option 6865i.cfg-server-address code 2 = string;
option 6865i.cfg-contact-rcs code 03 = boolean;
option 6865i.ActivateVLANHeader code 08 = text;
option 6865i.VLAN-ID code 09 = unsigned integer 32;

# Declaration of the terminal structure 6867i
option space 6867i;
option 6867i.cfg-server-address code 2 = string;
option 6867i.cfg-contact-rcs code 03 = boolean;
option 6867i.ActivateVLANHeader code 08 = text;
option 6867i.VLAN-ID code 09 = unsigned integer 32;

# Declaration of the terminal structure 6869i
option space 6869i;
option 6869i.cfg-server-address code 2 = string;
option 6869i.cfg-contact-rcs code 03 = boolean;
option 6869i.ActivateVLANHeader code 08 = text;
option 6869i.VLAN-ID code 09 = unsigned integer 32;

# Declaration of the terminal structure 6873i
option space 6873i;
option 6873i.cfg-server-address code 2 = string;
option 6873i.cfg-contact-rcs code 03 = boolean;
option 6873i.ActivateVLANHeader code 08 = text;
option 6873i.VLAN-ID code 09 = unsigned integer 32;

class "6735i" {
  match if substring(option vendor-class-identifier,0,18) = "AastraIPPhone6735i";
}
# End of class

class "6737i" {
  match if substring(option vendor-class-identifier,0,18) = "AastraIPPhone6737i";
}
# End of class

class "6863i" {
  match if substring(option vendor-class-identifier,0,18) = "AastraIPPhone6863i";
}
# End of class


class "6865i" {
  match if substring(option vendor-class-identifier,0,18) = "AastraIPPhone6865i";
}
# End of class

class "6867i" {
  match if substring(option vendor-class-identifier,0,18) = "AastraIPPhone6867i";
}
# End of class

class "6869i" {
  match if substring(option vendor-class-identifier,0,18) = "AastraIPPhone6869i";
}
# End of class

class "6873i" {
  match if substring(option vendor-class-identifier,0,18) = "AastraIPPhone6873i";
```

```
}
# End of class

# Declaring VLAN1 subnet
subnet 10.1.1.0 netmask 255.255.255.0 {
interface eth0;
option subnet-mask 255.255.255.0 ;
default-lease-time 1209600 ;
max-lease-time 1209600 ;
option routers 10.1.1.254 ;
option time-offset -3600 ;

pool {
allow members of "6735i";
allow members of "6737i";
allow members of "6863i";
allow members of "6865i";
allow members of "6867i";
allow members of "6869i";
allow members of "6873i";
range 10.1.1.100 10.1.1.109;

if substring(option vendor-class-identifier,0,18) = "AastraIPPhone6735i" {
# dhcp parameters specific to the subnet and to the terminal 6735i

option server.vendor-option-space 6735i;
option 6735i.cfg-server-address "ftp://connexio:connexio@50.1.1.1";
option 6735i.cfg-contact-rcs false;
option 6735i.ActivateVLANHeader "Aastra Telecom ";
option 6735i.VLAN-ID 100;
}
# End of pool condition

if substring(option vendor-class-identifier,0,18) = "AastraIPPhone6737i" {
# dhcp parameters specific to the subnet and to the terminal 6737i

option server.vendor-option-space 6737i;
option 6737i.cfg-server-address "ftp://connexio:connexio@50.1.1.1";
option 6737i.cfg-contact-rcs false;
option 6737i.ActivateVLANHeader "Aastra Telecom ";
option 6737i.VLAN-ID 100;
}
# End of pool condition

if substring(option vendor-class-identifier,0,18) = "AastraIPPhone6863i" {
# dhcp parameters specific to the subnet and to the terminal 6863 SIP

option server.vendor-option-space 6863i;
option 6863i.cfg-server-address "ftp://connexio:connexio@50.1.1.1";
option 6863i.cfg-contact-rcs false;
option 6863i.ActivateVLANHeader "Aastra Telecom ";
option 6863i.VLAN-ID 100;
}
# End of pool condition

if substring(option vendor-class-identifier,0,18) = "AastraIPPhone6865i" {
# dhcp parameters specific to the subnet and to the terminal 6865 SIP

option server.vendor-option-space 6865i;
```

```
option 6865i.cfg-server-address "ftp://connexio:connexio@50.1.1.1";
option 6865i.cfg-contact-rcs false;
option 6865i.ActivateVLANHeader "Aastra Telecom ";
option 6865i.VLAN-ID 100;
}
# End of pool condition

if substring(option vendor-class-identifier,0,18) = "AastraIPPhone6867i" {
# dhcp parameters specific to the subnet and to the terminal 6867i

option server.vendor-option-space 6867i;
option 6867i.cfg-server-address "ftp://connexio:connexio@50.1.1.1";
option 6867i.cfg-contact-rcs false;
option 6867i.ActivateVLANHeader "Aastra Telecom ";
option 6867i.VLAN-ID 100;
}
# End of pool condition

if substring(option vendor-class-identifier,0,18) = "AastraIPPhone6869i" {
# dhcp parameters specific to the subnet and to the terminal 6869i

option server.vendor-option-space 6869i;
option 6869i.cfg-server-address "ftp://connexio:connexio@50.1.1.1";
option 6869i.cfg-contact-rcs false;
option 6869i.ActivateVLANHeader "Aastra Telecom ";
option 6869i.VLAN-ID 100;
}
# End of pool condition

if substring(option vendor-class-identifier,0,18) = "AastraIPPhone6873i" {
# dhcp parameters specific to the subnet and to the terminal 6873i

option server.vendor-option-space 6873i;
option 6873i.cfg-server-address "ftp://connexio:connexio@50.1.1.1";
option 6873i.cfg-contact-rcs false;
option 6873i.ActivateVLANHeader "Aastra Telecom ";
option 6873i.VLAN-ID 100;
}
# End of pool condition

}
# End of pool

}
# End of subnet
#End of configuration file
```

- In this other example, Mitel 6000 SIP phones negotiate VLAN ID 8 via option 132, and the RCS option is disabled.



**ATTENTION : The Vendor Class of Mitel 6000 SIP phones is tested in this example on the first 13 characters of the Vendor Class, which facilitates the configuration file.**

```
ddns-update-style none;
authoritative;

# Declaring the structure of Mitel 6000 SIP Phone, modele all_models
option space Connexio-all;
option Connexio-all.contact-rcs code 3 = boolean;
option Connexio-all.cfg-server-address code 2 = string;
option vlan-id code 132 = unsigned integer 16;

class "6xxxi all_models" {
  match if substring(option vendor-class-identifier,0,13) = "AastraIPPhone";

}
# End of class

# Declaring the subnet
subnet 20.1.1.0 netmask 255.255.255.0 {
  interface eth0;
  default-lease-time 1209600 ;
  max-lease-time 1209600 ;
  option routers 20.1.1.254 ;

  pool {
    allow members of "6xxxi all_models";
 range 20.1.1.100 20.1.1.199;

    if substring(option vendor-class-identifier,0,13) = "AastraIPPhone" {
      # Special DHCP parameters for the subnet and 6xxxi all_models
      option vlan-id 8 ;

      option server.vendor-option-space Connexio-all;
      option Connexio-all.contact-rcs false;
      option Connexio-all.cfg-server-address "ftp://connexio:connexio@20.1.1.2";
    }
    # End of pool condition
}
  # End of pool
}
# End of subnet
#End of configuration file
```

### 2. Configuration file consistency check

A command is used to check the consistency of the configuration file. If a parameter is wrongly configured, this command identifies the incorrect line as well as the type of error concerned.

- In a terminal window, type in the command:

dhcpd -t
Example of error message:

```
[root@aamadeus1 ~]# dhcpd -t
Internet Systems Consortium DHCP Server V3.0.5-RedHat
Copyright 2004-2006 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/
/etc/dhcpd.conf line 210: expecting string.
      option tftp-server-name 10.
                              ^
Configuration file errors encountered -- exiting
```

### 3. Starting the dhcpd service.

Select Menu **System > Administration > Server parameters > Services.**

Select the dhcpd service and click Start.

# 10.2 CONFIGURING THE EXTERNAL DHCP SERVER FOR MIVOICE 5300 IP PHONES

## 10.2.1 STANDARD DHCP SETTINGS OR OPTIONS MANAGED BY MIVOICE 5300 IP PHONE,

MiVoice 5300 IP Phone contains two distinct DHCP clients, one associated with the boot sequence, and the other with the terminal application start. The appended table describes the options managed by the terminal according to the requested DHCP client.

| STANDARD DHCP PARAMETERS OR OPTIONS | USED BY | PROTECTION(1) | NOTE: |
|---|---|---|---|
| IP address and subnet mask (option 1) | Boot<br>Application | Yes | parameter required in option 55 |
| Gateway IP address (option 3) | Boot<br>Application | Yes | parameter required in option 55 |
| DNS server IP address (option 6) | Application | Yes | parameter required in option 55 |
| DNS domain name (option 15) | Application | NA | parameter required in option 55 |
| Transmission address (option 28) | Application | NA | parameter required in option 55 |
| Vendor-specific option (option 43) | Application | NA | parameter required in option 55 |
| FTP server IP address (option 66) | Boot | No | Accepted if the flash value is the default value or 0.0.0.0 |
| Name of firmware to download (option 67) | Boot | No | Accepted if the value in flash is the default value and if the firmware name starts with “aamxip” |

(1) protection against manual write from the terminal or web interface if DHCP mode is enabled

### 10.2.2 SPECIFIC DHCP SETTINGS MANAGED BY MIVOICE 5300 IP PHONES VIA OPTION 43

MiVoice 5300 IP Phones send option 60 of the DHCP protocol (vendor class identifier) in the DHCP request (discover/request) to identify themselves as an **Aamadeus IP Phone**. This identifier is the same for the four terminal models: 5360 IP, 5361ip, 5370 IP and 5380 IP.

Moreover, MiVoice 5300 IP Phones prompt the DHCP server for vendor specific information, by specifying option 43 in their list of requests for parameters associated with option 55.

If the DHCP server is configured to react to the vendor specific identifier, it will add option 43 (vendor specific information) to these replies.

The table below describes all the parameters that can be negotiated via option 43:

| PARAMETER | CODE | HEX. VALUE | LENGTH/ TYPE | NOTE: |
|---|---|---|---|---|
| PBX_ADDRESS | 10/03 | 10/03 | 04/IP addr | Specifies the SIP gateway main IP address |
| SIP_PORT_PBX | 10/04 | 10/04 | 02/Word | Specifies the listening SIP port of the main system |
| SIP_PORT_PHONE | 10/05 | 10/05 | 02/Word | Specifies the listening SIP port of the terminal |
| VLAN_PRIO | 10/07 | 10/07 | 01/Byte | Specifies the terminal's VLAN port priority |
| VLAN_ID/VLAN_ENABLED | 10/08 | 10/08 | 02/Word | Specifies the VLAN ID used by the terminal's VLAN port. 0=port VLAN ToIP not enabled. If a value is defined, the terminal VLAN marking is enabled (**code 7 required**). |
| VLANPC_PRIO | 10/09 | 10/09 | 01/Byte | Specifies the PC VLAN port priority |
| VLANPC_ID/VLANPC_ENABLED | 10/10 | 0A | 02/Word | Specifies the VLAN ID used by the PC port. 0=port VLAN PC not activated (**code 9 required**) |
| VLANPC_TAGS | 10/11 | 0B | 01/Byte | Specifies whether the VLAN ID marking used by the PC port is enabled (1) or not (0) |
| PBX_ADDRESS_BACKUP | 10/19 | 10/13 | 04/IP addr | Specifies the SIP gateway secondary IP address(1) |
| SIP_PORT_PBX_BACKUP | 10/20 | 10/14 | 02/Word | Specifies the listening SIP port of the secondary system(1) |

**Note : (1) Used as of version V5.1B for the dual homing function.**

**ATTENTION : Codes 07 and 08 must be negotiated together.**

**ATTENTION : Codes 09 and 10 must be negotiated together.**

## 10.2.3 CONFIGURING A DHCP SERVER ON A PLATFORM WINDOWS 2000/2003

### *10.2.3.1 Configuring standard network parameters from the DHCP server*

By default, the terminal is set to active DHCP (enabled).

Principle

The first time it is connected, the terminal makes a DHCP request to all the DATA defined on the DHCP server. This DATA on the DHCP server must contain the following options:

- Standard Option 03: router (gateway) IP address
- Standard Option 66: FTP server IP address
- Standard Option 67*: name of terminal firmware to download

**Note : * If the beginning of the default firmware name (aamxip_v*.ftp) is the same as the one available in the FTP server storage area, this option is not obligatory.**

And possibly the following two options:

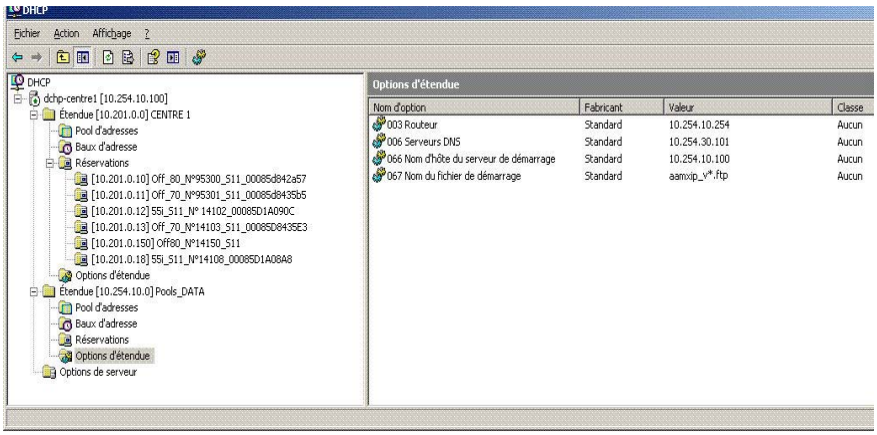
- Specification Option 07 "Aamadeus IP Phone" ** : terminal VLAN priority
- Specification Option 08 "Aamadeus IP Phone" ** : terminal VLAN number

**Note : ** These two options can be negotiated directly by MiVoice 5300 IP Phone with the DHCP server in the DATA range, which enables data applications to use standard option 67 freely in this range.**

The IP address range associated with the DATA range must be enough to provide a temporary IP address to each MiVoiceMiVoice 5300 IP Phone when it is first installed on the LAN.

During this first transaction with the DHCP server in the DATA VLAN, the DHCP server assigns to each terminal:

- A temporary IP address
- Its temporary subnet mask
- The DATA subnet gateway (router) IP address
- The FTP server IP address
- The name of terminal firmware to download.




This first DHCP transaction in the DATA range enables MiVoice 5300 IP Phone to update its firmware with the latest release compatible with the MiVoice 5000 solution, to correctly initialise MiVoice 5300 IP Phone (file **tm.config.<TT>.<VN>.ftp)** and recover all the network parameters it requires to work well, via

the global and specific configuration files . These files are provided manually in the FTP server storage area and downloaded from the FTP server.

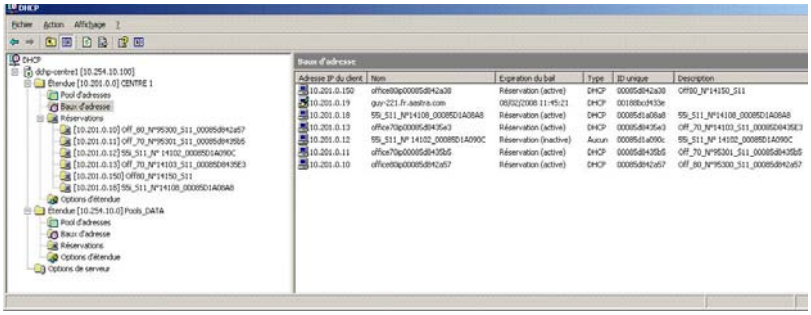
The global and specific configuration files allow the terminal, among other things, to retrieve its terminal VLAN ID with its associated priority if these parameters have not been negotiated with the DHCP server. After this modification, the terminal will restart to take into account these new network parameters, and the temporary IP address taken by the terminal will be released.

When MiVoice 5300 IP Phone is started for a second time, the terminal makes a second DHCP transaction by querying the MiVoice 5300 IP Phone TERMINAL range defined on the DHCP server. This MiVoice 5300 IP Phone TERMINAL range on the DHCP server must contain the following options:

- Standard option 03: Router (gateway) IP address
- Standard option 66: FTP server IP address
- Standard option 67*: name of the terminal firmware to download.

**Note : * If the beginning of the default firmware name (aamxip_v*.ftp) is the same as the one available in the FTP server storage area, this option is not obligatory.**

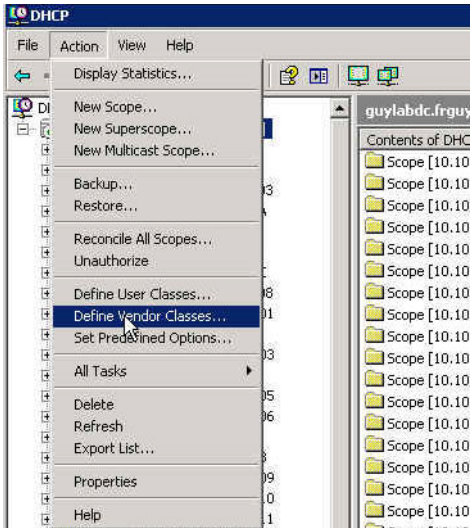
Standard Options 66 and 67 can be associated either with the full range or on terminal basis by creating IP address reservations from the MAC addresses of each MiVoice 5300 IP Phone. This reservation from MAC addresses may become obligatory if different terminal models are combined in the same range (the same subnet) and do not use the same FTP server.



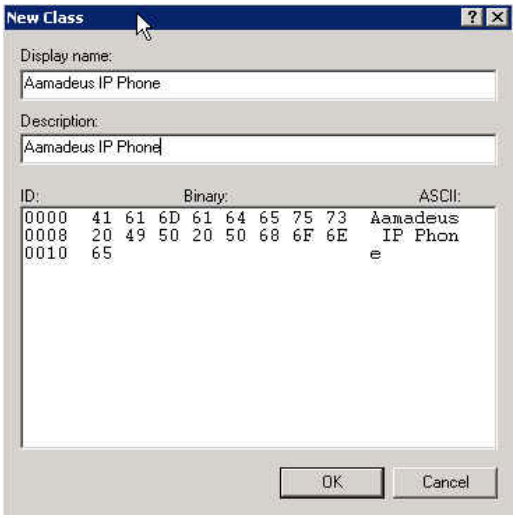
### 10.2.3.2 Configuring the vendor class and options associated with the DHCP server

In the DHCP server management interface:

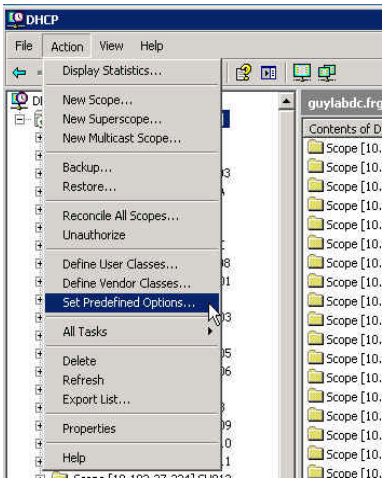
Select the column Action/Define Vendor Classes




In the following window, enter in the ASCII area the value “Aamadeus IP Phone” corresponding to the MiVoice 5300 IP Phone identifier.



Then select the column Action/Set Predefined Options.




Select the vendor class “Aamadeus IP Phone” in the “Option Class” field then click Add. Enter:

- The name of the option to be created: PBX_ADDRESS
- Type of data: IP address
- The code associated with the option: 10/03
- The description associated with the option: PBX_ADDRESS

The possible values of the first three fields are defined in the table “Standard DHCP settings or options managed by MiVoice 5300 IP Phone,”, page 305. Confirm the creation by pressing OK.

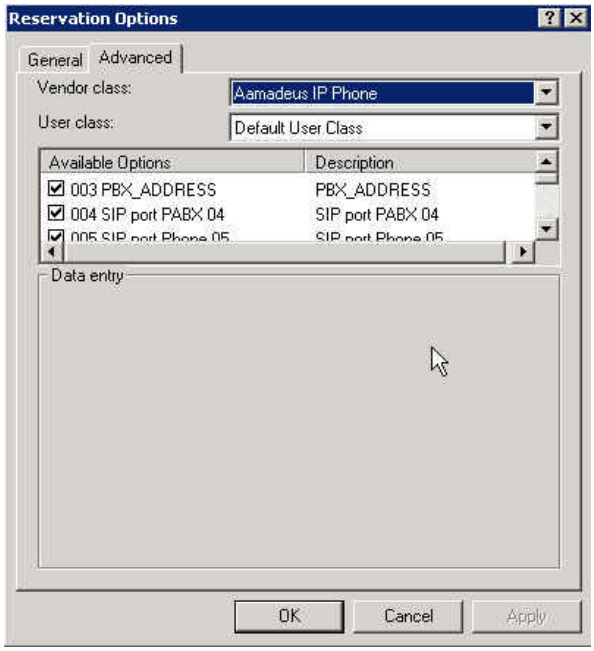


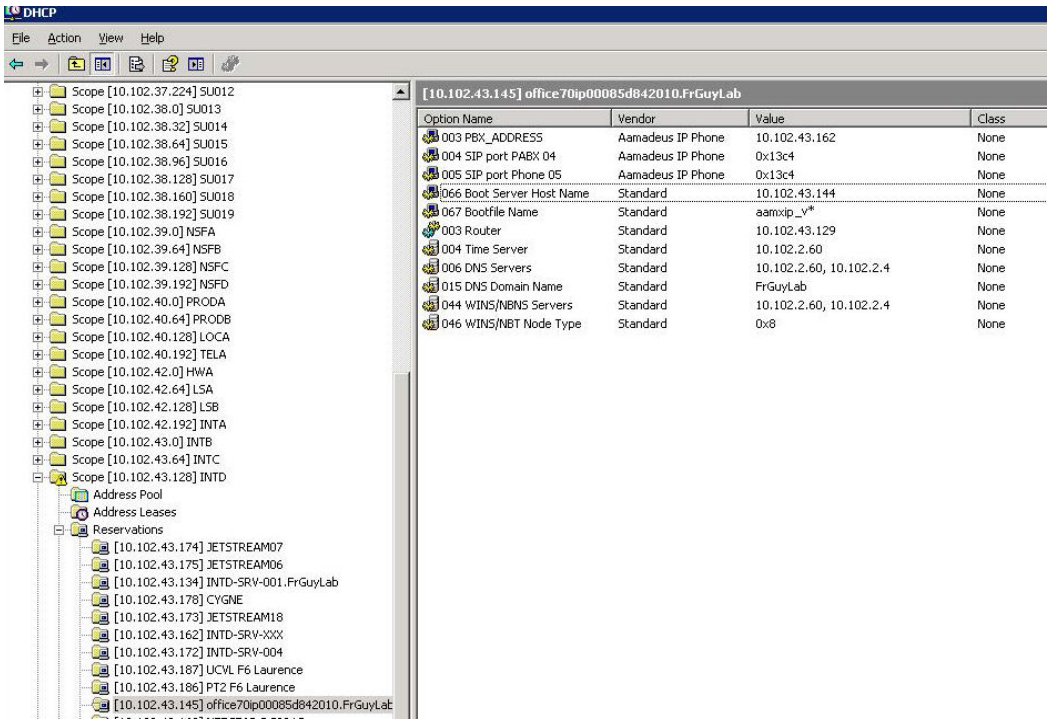

Return to the predefined options and values menu, then select the option just created to enter its default value  in the value field:




All the options defined for this class (vendor class) can be associated with all the DHCP server scopes (global options scope), with a specific scope (subnet options scope) or a specific terminal (configuration

options of the reservation associated with the terminal) using the “Advanced” tab of the “Reservation Options” menu.



### 10.2.4 CONFIGURING A DHCP SERVER ON A MIVOICE 5000 SERVER PLATFORM FOR MIVOICE 5300 IP PHONES

The procedure for configuring a DHCP server on a LINUX platform is the same as the one described in Chapter 10.2.3.



**ATTENTION : UDP ports 67 and 68 must be open if the A5MiVoice 5000 Server firewall is enabled.**

In the example below, the DHCP server used is dhcpd. This package is not installed by default when RedHat Enterprise 5 is installed on the MiVoice 5000 Server platform. The installation of this package is described in the Appendix.

Proceed as follows:

**1. Configure the configuration file dhcpd.conf available in the directory /etc.**

The modifications consist in:

- Define all the vendor codes that can be used by MiVoice 5300 IP Phones.
- Define standard options 03, 66 and 67 for each ToIP subnet.
- If necessary, define for each ToIP subnet concerned the MAC-address-based reservations for MiVoice 5300 IP Phones with the vendor options possibly used.

The file dhcpd.conf below is a non-exhaustive example of a typical configuration, including all Mitel MiVoice 5300 IP Phones.

```
# Configuration file generated on 28/07/2008
ddns-update-style none;
authoritative;

# Declaring the structure of MiVoice 5300 IP Phone, modele 60ip-70ip-80ip
option space Office-ip;
option Office-ip.primary-pbx-address code 3 = ip-address;
option Office-ip.pbx-sip-port code 4 = unsigned integer 16;
option Office-ip.ip-phone-sip-port code 5 = unsigned integer 16;
option Office-ip.phone-vlan-priority code 7 = unsigned integer 8;
option Office-ip.phone-vlan-id code 8 = unsigned integer 16;
option Office-ip.pc-vlan-priority code 9 = unsigned integer 8;
option Office-ip.pc-vlan-id code 10 = unsigned integer 16;
option Office-ip.pc-vlan-tags code 11 = unsigned integer 8;
option Office-ip.sip-port-backup code 20 = unsigned integer 16;
option Office-ip.secondary-pbx-address code 19 = ip-address;


class "MiVoice 5300 IP Phone 60ip-70ip-80ip" {
match if substring(option vendor-class-identifier,0,17) = "Aamadeus IP Phone";
}
# End of class


# Declaring VLAN1 subnet
subnet 10.1.1.0 netmask 255.255.255.0 {
interface eth0;
option subnet-mask 255.255.255.0 ;
default-lease-time 1209600 ;
max-lease-time 1209600 ;
option routers 10.1.1.254 ;
option time-offset -3600 ;
```

```
pool {
allow members of "MiVoice 5300 IP Phone 60ip-70ip-80ip";
range 10.1.1.100 10.1.1.199;


if substring(option vendor-class-identifier,0,17) = "Aamadeus IP Phone" {
# Special DHCP parameters for the subnet and MiVoice 5300 IP Phone 60ip-70ip-80ip
option tftp-server-name "50.1.1.1" ;
option bootfile-name "aamxip_v*.ftp" ;
option domain-name "fr.aastra.com" ;
option domain-name-servers 20.1.1.50 ;
option broadcast-address 10.1.1.255 ;

option server.vendor-option-space Office-ip;
option Office-ip.primary-pbx-adress 50.1.1.1;
option Office-ip.pbx-sip-port 5060;
option Office-ip.ip-phone-sip-port 5060;
option Office-ip.phone-vlan-priority 6;
option Office-ip.phone-vlan-id 1;
option Office-ip.pc-vlan-priority 0;
option Office-ip.pc-vlan-id 2;
option Office-ip.pc-vlan-tags 0;
}
# End of pool condition

}
# End of pool
}
# End of subnet
#End of configuration file
```

### 2. Configuration file consistency check

A command is used to check the consistency of the configuration file. If a parameter is wrongly configured, this command identifies the incorrect line as well as the type of error concerned.

- In a terminal window, type in the command:

```
dhcpd -t
```

Example of error message:

```
[root@aamadeus1 ~]# dhcpd -t
Internet Systems Consortium DHCP Server V3.0.5-RedHat
Copyright 2004-2006 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/
/etc/dhcpd.conf line 210: expecting string.
      option tftp-server-name 10.
Configuration file errors encountered -- exiting
```

### 3. Starting the dhcpd service.

Select Menu **System > Administration > Server parameters > Services.**

Select the dhcpd service and click Start.

## 10.3 CONFIGURING THE EXTERNAL DHCP SERVICE IN A REDUNDANT MIVOICE 5000 SERVER CONFIGURATION

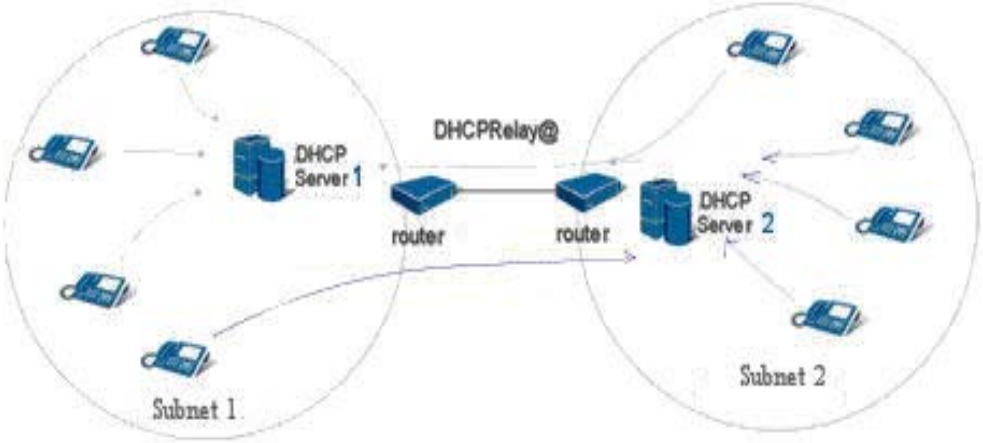
Two external DHCP servers can be activated simultaneously to duplicate the DHCP service.

Each DHCP server (1 & 2) must be able to provide IP addresses for all MiVoice 5300 IP Phones and Mitel 6000 SIP Phones on each site. For this, each site's IP subnet declaration will be shared between the two DHCP servers in order to avoid IP address duplication. The number of available IP addresses per server must be enough to provide the required amount if any of the two DHCP servers fails.

**ATTENTION : For the DHCP request sent by a terminal to be processed correctly, a DHCP RELAY function is implemented on each router setting up connection to the terminal VLAN on the site. The DHCP request must be sent to the two DHCP servers installed and configured on each MiVoice 5000 Server platform.**
**The DHCP service is external. It is neither installed nor managed by the MiVoice 5000 Server Web Admin.**

| VLAN | Relay | DHCP server |
|---|---|---|
| 1 | DHCPRelay1 | DHCP 2 |

| VLAN | Relay | DHCP server |
|---|---|---|
| 2 | DHCPRelay2 | DHCP 1 |



# 11 CONFIGURING THE FTP SERVERS USED BY TMA

## 11.1 CONFIGURING AN FTP SERVER ON A PLATFORM WINDOWS 2000/ 2003 FOR MIVOICE 5300 IP PHONES

The mandatory prerequisite is that the FTP server manages passive mode. In the example below, the FTP server used is Filezilla Server.

### 11.1.1 ACCOUNTS ASSOCIATED WITH THE STORAGE DIRECTORIES FOR MIVOICE 5300 IP PHONES

**Tableau 11.1 :**

| DEDICATED DIRECTORIES * | RIGHT | LOGIN | PASSWORD |
|---|---|---|---|
| /opt/a5000/infra/sip_sets/53xxip<br>Production release | Read/Write via FTP | mngt_ftp_53xxip | mngt_ftp_53xxip |
| /opt/a5000/infra/sip_sets/53xxip<br>Production release | Reading via FTP | aamadeus | aamadeus |
| /opt/a5000/infra/sip_sets/<br>test_53xxip<br>Test version | Read/Write via FTP | mngt_test_53xxip | mngt_test_53xxip |
| /opt/a5000/infra/sip_sets/<br>test_53xxip<br>Test version | Reading via FTP | test_aamadeus | test_aamadeus |

* : In the column **Dedicated directories**, the directory tree is free **but** the definition of accounts must be fully consistent with the ones defined in TMA.

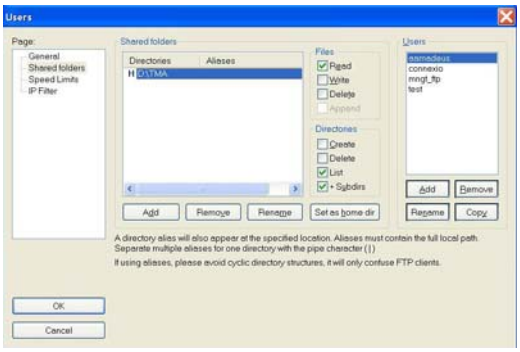
In this same column, the tree is given as an example and corresponds to the one imposed for integrated TMA.

### 11.1.2 CREATING THE ACCOUNT USED BY TERMINALS FOR THE PRODUCTION VERSION

This account enables MiVoice 5300 IP Phones to access the storage directory in which the terminal software and all the configuration files for the production version are located.

**ATTENTION : This account must also be defined in TMA, in the FTP server configuration menu.**

- Select Menu **Edit > Users > General.**
- Click **Add** to create a new user account.
- Enter the name of the account: **aamadeus** and click OK to confirm.
- For the **aamadeus** account, tick the password box and enter the associated password: **aamadeus**. Click OK to confirm.
- Select Menu **Edit > Users > Shared folders.**
- In the Shared folders area, click **Add** to associate the storage directory with the **aamadeus** account. Tick the options used to obtain read-only rights.




- Click OK to confirm the selection. Click OK to confirm these changes.

**ATTENTION : The login and password used by MiVoice 5300 IP Phones in the production version must be "aamadeus".**

### 11.1.3 CREATING THE ACCOUNT USED BY TERMINALS FOR THE TEST VERSION

This account enables MiVoice 5300 IP Phones to access the storage directory in which the terminal software and all the configuration files for the test version are located.

**ATTENTION : This account must also be defined in TMA, in the FTP server configuration menu.**

- Select Menu **Edit > Users > General.**
- Click **Add** to create a new user account.
- Enter the name of the account: **test_aamadeus** and click OK to confirm.
- For the test account, tick the password box and enter the associated password: **test_aamadeus**. Click OK to confirm.

- Select Menu **Edit > Users > Shared folders.**
- In the Shared folders area, click **Add** to associate the right storage directory with the **test_aamadeus** account. Tick the options used to obtain read-only rights.
- Click OK to confirm the selection. Click OK to confirm these changes.

### 11.1.4 CREATING THE ACCOUNT USED BY TMA (PRODUCTION VERSION)

This account enables the TMA application to place in the **Production version** directory the terminal software and configuration files for MiVoice 5300 IP Phone.



**ATTENTION : This account must also be defined in TMA, in the FTP server configuration menu.**

**For the production version account mngt_ftp_53xxip**

- Select Menu **Edit > Users > General.**
- Click **Add** to create a new user account.
- Enter the name of the account: **mngt_ftp_53xxip** then click OK to confirm.
- For the account **mngt_ftp_53xxip**, tick the password box and enter the associated password: **mngt_ftp_53xxip**then click OK to confirm.
- Select Menu **Edit > Users > Shared folders.**
- In the Shared folders area, click **Add** to associate the right storage directory with the **mngt_ftp_53xxip** account. Tick the options used to have read / write / delete rights.
- Click OK to confirm the selection. Click OK to confirm these changes.

### 11.1.5 CREATING THE ACCOUNT USED BY TMA (TEST VERSION)

This account enables the TMA application to place in the **Test version** directory the terminal software and configuration files for MiVoice 5300 IP Phone.



**ATTENTION : This account must also be defined in TMA, in the FTP server configuration menu.**

**For the test version** account **mngt_test_53xxip**

- Select Menu **Edit > Users > General.**
- Click **Add** to create a new user account.
- Enter the name of the account: **mngt_test_53xxip** then click OK to confirm.
- For the account **mngt_test_53xxip**, tick the password box and enter the associated password: **mngt_test_53xxip**. Click OK to confirm.
- Select Menu **Edit > Users > Shared folders.**
- In the Shared folders area, click **Add** to associate the right storage directory with the **mngt_test_53xxip** account. Tick the options used to have read / write / delete rights.
- Click OK to confirm the selection. Click OK to confirm these changes.

## 11.2 CONFIGURING AN FTP SERVER ON A MIVOICE 5000 SERVER PLATFORM FOR MIVOICE 5300 IP PHONES

The mandatory prerequisite is that the FTP server manages passive mode.

**ATTENTION : TCP port 21 must be open if the MiVoice 5000 Server firewall is enabled.**

In the example below, the FTP server used is **vsftpd**. This package is installed by default when RedHat Enterprise 5 is installed on the MiVoice 5000 Server platform.

### 11.2.1 ACCOUNTS ASSOCIATED WITH THE STORAGE DIRECTORIES FOR MIVOICE 5300 IP PHONES

**Tableau 11.2 :**

| DEDICATED DIRECTORIES * | RIGHT | LOGIN | PASSWORD |
|---|---|---|---|
| /opt/a5000/infra/sip_sets/53xxip<br>Production release | Read/Write via FTP | mngt_ftp_53xxip | mngt_ftp_53xxip |
| /opt/a5000/infra/sip_sets/53xxip<br>Production release | Reading via FTP | aamadeus | aamadeus |
| /opt/a5000/infra/sip_sets/<br>test_53xxip<br>Test version | Read/Write via FTP | mngt_test_53xxip | mngt_test_53xxip |
| /opt/a5000/infra/sip_sets/<br>test_53xxip<br>Test version | Reading via FTP | test_aamadeus | test_aamadeus |

* : In the column **Dedicated directories**, the directory tree is free **but** the definition of accounts must be fully consistent with the ones defined in TMA.

In this same column, the tree is given as an example and corresponds to the one imposed for integrated TMA.

**ATTENTION : As of MiVoice 5000 R5.2 SP1 on MiVoice 5000 Server, the FTP service may be installed and managed via Web Admin. In that case, the accounts used by MiVoice 5300 IP Phones are automatically defined as described in the above table at the start of the FTP service (automatic start using Ctrl I or manually via Web Admin).**
**The rights associated with these accounts, as well as their storage directory, are also automatically created as described in the next chapters.**

### 11.2.2 CREATING THE ACCOUNT USED BY TERMINALS FOR THE PRODUCTION VERSION

This account has read-only rights and enables MiVoice 5300 IP Phones to access the storage directory in which the terminal software and all the configuration files for the production version are located.

- Select Menu **System > Administration > Users and groups**.
- Click **Add user**.

In the screen that opens:

- Enter the user name: **aamadeus**
- Enter the full name: **aamadeus**
- Enter the password: **aamadeus**
- Confirm the password: **aamadeus**
- Indicate the connection shell: **/bin/bash**
- Tick the box **create a personal directory** and enter it (for instance the one used for integrated TMA): **/opt/a5000/infra/sip_sets/53xxip**
- Untick the creation of a private group for the user.
- Click **Confirm** to confirm these parameters.

**ATTENTION : The login and password used by MiVoice 5300 IP Phones in the production version must be "aamadeus".**

### 11.2.3 CREATING THE ACCOUNT USED BY TERMINALS FOR THE TEST VERSION

This account has read-only rights and enables MiVoice 5300 IP Phones to access the storage directory in which the terminal software and all the configuration files in test mode are located.

- Select Menu **System > Administration > Users and groups**.
- Click **Add user**.

In the screen that opens:

- Enter the user name: **test_aamadeus**
- Enter the full name: **test_aamadeus**
- Enter the password: **test_aamadeus**
- Confirm the password: **test_aamadeus**
- Indicate the connection shell: **/bin/bash**
- Tick the box **create a personal directory** and enter it (for instance the one used for integrated TMA): **/opt/a5000/infra/sip_sets/test_53xxip**
- Untick the creation of a private group for the user.
- Click Validate to confirm these parameters.

**Note : The login and password are provided as example.**

### 11.2.4 CREATING THE ACCOUNT USED BY TMA (PRODUCTION VERSION)

This account has read/write rights and enables the TMA application to place in the production directory the terminal software and configuration files for MiVoice 5300 IP Phones.

- Select Menu **System > Administration > Users and groups**.
- Click **Add user**.

In the screen that opens:

- Enter the user name: **mngt_ftp_53xxip**
- Enter the full name: **mngt_ftp_53xxip**
- Enter the password: **mngt_ftp_53xxip**
- Confirm the password: **mngt_ftp_53xxip**
- Indicate the connection shell: **/bin/bash**
- Tick the box **create a personal directory** and enter it (for instance the one used for integrated TMA): **/opt/a5000/infra/sip_sets/53xxip**
- Untick the creation of a private group for the user.
- Click Validate to confirm these parameters.

### 11.2.5 CREATING THE ACCOUNT USED BY TMA (TEST VERSION)

This account has read/write rights and enables the TMA application to place in the test directory the terminal software and configuration files for MiVoice 5300 IP Phones.

**For the production version**

- Select Menu **System > Administration > Users and groups**.
- Click **Add user**.

In the screen that opens:

- Enter the user name: **mngt_test_53xxip**
- Enter the full name: **mngt_test_53xxip**
- Enter the password: **mngt_test_53xxip**
- Confirm the password: **mngt_test_53xxip**
- Indicate the connection shell: **/bin/bash**
- Tick the box **create a personal directory** and enter it (for instance the one used for integrated TMA): **/opt/a5000/infra/sip_sets/test_53xxip.**



**ATTENTION : These four accounts must also be defined in TMA.**

### 11.2.6 CREATING THE MNGT_FTP_53XXIP GROUP

This group has read / write rights and is used to assign the appropriate rights to the **aamadeus** and **mngt_ftp_53xxip** account.

- Select Menu **System > Administration > Users and groups**.
- Click **Add group**.
- Enter the name of the group: **mngt_ftp_53xxip**
- Click Validate to confirm these parameters.

### 11.2.7 CREATING THE MNGT_TEST_53XXIP GROUP

This group has read / write rights and is used to assign the appropriate rights to the **test_aamadeus** and **mngt_ftp_53xxip** account.

- Select Menu **System > Administration > Users and groups**.
- Click **Add group**.
- Enter the name of the group: **mngt_test_53xxip**
- Click Validate to confirm these parameters.

### 11.2.8 CHANGE THE OWNER AND GROUP ASSOCIATED WITH THE MIVOICE 5300 IP PHONE.

Open a terminal window then go to **/opt/a5000/infra/sip_sets** (using the example used from the integrated TMA).

- Type in the following command:

  **chown aamadeus:mngt_ftp_53xxip 53xxip**

**ATTENTION : Respect he space before the last MiVoice 5300 IP Phone.**

### 11.2.9 MODIFY THE RIGHTS ASSOCIATED WITH THE MIVOICE 5300 IP PHONE DIRETORY.

Open a terminal window then go to **/opt/a5000/infra/sip_sets** (using the example used from the integrated TMA).

- Type in the following command:

  **chmod 577 53xxip**

### 11.2.10 CHANGE THE OWNER AND GROUP ASSOCIATED WITH THE TEST DIRECTORY.

Open a terminal window then go to **/opt/a5000/infra/sip_sets** (using the example used from the integrated TMA).

- Type in the following command:

  **chown test_aamadeus:mngt_test_53xxip test_53xxip**

### 11.2.11 CHANGE THE RIGHTS ASSOCIATED WITH THE TEST DIRECTORY.

Open a terminal window then go to /opt/a5000/infra/sip_sets (using the example used from the integrated TMA).

- Type in the following command:

  **chmod 577 test_53xxip**

### 11.2.12 MODIFY THE FILE VSFTPD.CONF UNDER /ETC/VSFTPD.

The modifications consist in:

- disallowing anonymous connections: you must connect to the FTP server with a user or system account (**anonymous_enable=NO)**.
- Limit the number of simultaneous connections to 1000 (**max_clients = 1000)**.

These modifications appear in bold in the file used as example below.

*# Example config file /etc/vsftpd/vsftpd.conf*
*#Beginning of the file*
*# The default compiled in settings are fairly paranoid. This sample file*
*# loosens things up a bit, to make the ftp daemon more usable.*
*# Please see vsftpd.conf.5 for all compiled in defaults.*
*#*
*# READ THIS: This example file is NOT an exhaustive list of vsftpd options.*
*# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's*
*# capabilities.*
*#*
*# Allow anonymous FTP? (Beware - allowed by default if you comment this out).*
***anonymous_enable=NO***
*#*
*# Uncomment this to allow local users to log in.*
*local_enable=YES*
*#*
*# Uncomment this to enable any form of FTP write command.*
*write_enable=YES*
*#*
*# Default umask for local users is 077. You may wish to change this to 022,*
*# if your users expect that (022 is used by most other ftpd's)*
*local_umask=022*
*#*
*# Uncomment this to allow the anonymous FTP user to upload files. This only*
*# has an effect if the above global write enable is activated. Also, you will*
*# obviously need to create a directory writable by the FTP user.*
*#anon_upload_enable=YES*
*#*
*# Uncomment this if you want the anonymous FTP user to be able to create*
*# new directories.*
*#anon_mkdir_write_enable=YES*
*# Activate directory messages - messages given to remote users when they*
*# go into a certain directory.*
*dirmessage_enable=YES*
*#*
*# Activate logging of uploads/downloads.*
*xferlog_enable=YES*
*#*
*# Make sure PORT transfer connections originate from port 20 (ftp-data).*
*connect_from_port_20=YES*
*# If you want, you can arrange for uploaded anonymous files to be owned by*
*# a different user. Note! Using "root" for uploaded files is not*
*# recommended!*
*#chown_uploads=YES*
*#chown_username=whoever*
*#*
*# You may override where the log file goes if you like. The default is shown*
*# below.*
*#xferlog_file=/var/log/vsftpd.log*

*#*
*# If you want, you can have your log file in standard ftpd xferlog format*
*xferlog_std_format=YES*
*#*
*# You may change the default value for timing out an idle session.*
*#idle_session_timeout=600*
*#*
*# You may change the default value for timing out a data connection.*
*#data_connection_timeout=120*
*#*
*# It is recommended that you define on your system a unique user which the*
*# ftp server can use as a totally isolated and unprivileged user.*
*#nopriv_user=ftpsecure*
*#*
*# Enable this and the server will recognise asynchronous ABOR requests. Not*
*# recommended for security (the code is non-trivial). Not enabling it,*
*# however, may confuse older FTP clients.*
*#async_abor_enable=YES*
*#*
*# By default the server will pretend to allow ASCII mode but in fact ignore*
*# the request. Turn on the below options to have the server actually do ASCII*
*# mangling on files when in ASCII mode.*
*# Beware that on some FTP servers, ASCII support allows a denial of service*
*# attack (DoS) via the command "SIZE /big/file" in ASCII mode. vsftpd*
*# predicted this attack and has always been safe, reporting the size of the*
*# raw file.*
*# ASCII mangling is a horrible feature of the protocol.*
*#ascii_upload_enable=YES*
*#ascii_download_enable=YES*
*#*
*# You may fully customise the login banner string:*
*#ftpd_banner=Welcome to blah FTP service.*
*#*
*# You may specify a file of disallowed anonymous e-mail addresses. Apparently*
*# useful for combatting certain DoS attacks.*
*#deny_email_enable=YES*
*# (default follows)*
*#banned_email_file=/etc/vsftpd/banned_emails*
*#*
***# Limitation of the number of simultaneous connections***
***max_clients=1000***
*#*
*# You may specify an explicit list of local users to chroot() to their home*
*# directory. If chroot_local_user is YES, then this list becomes a list of*
*# users to NOT chroot().*
*chroot_local_user=NO*
*#chroot_list_enable=YES*
*# (default follows)*
*#chroot_list_file=/etc/vsftpd/chroot_list*
*#*
*# You may activate the "-R" option to the builtin ls. This is disabled by*
*# default to avoid remote users being able to cause excessive I/O on large*
*# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume*
*# the presence of the "-R" option, so there is a strong case for enabling it.*
*#ls_recurse_enable=YES*
*#*
*# When "listen" directive is enabled, vsftpd runs in standalone mode and*
*# listens on IPv4 sockets. This directive cannot be used in conjunction*
*# with the listen_ipv6 directive.*

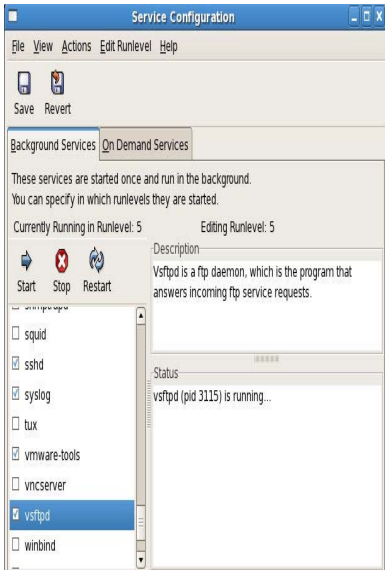
*listen=YES*
*#*
*# This directive enables listening on IPv6 sockets. To listen on IPv4 and IPv6*
*# sockets, you must run two copies of vsftpd whith two configuration files.*
*# Make sure, that one of the listen options is commented !!*
*#listen_ipv6=YES*
*pam_service_name=vsftpd*
*userlist_enable=YES*
*#userlist_file=/etc/vsftpd/user_list*
*tcp_wrappers=YES*
*#End of file.*

Concerning the line:
***# Limitation of the number of simultaneous connections***
***max_clients=1000***

- Then start the **vsftpd** service.

Select Menu **System > Administration > Server parameters > Services.**

Select the **vsftps** service and click **Start**.



## 11.3 CONFIGURING AN FTP SERVER ON A PLATFORM WINDOWS 2000/ 2003 FOR MITEL 6000 SIP PHONES

The mandatory prerequisite is that the FTP server manages passive mode.

### 11.3.1 ACCOUNTS ASSOCIATED WITH THE STORAGE DIRECTORIES FOR MITEL 6000 SIP PHONES

**Tableau 11.3 :**

| DEDICATED DIRECTORIES * | RIGHT | LOGIN | PASSWORD |
|---|---|---|---|
| /opt/a5000/infra/sip_sets/deploy-ment_67xxi<br>Production release for deployment | Reading via FTP | connexio | connexio |
| /opt/a5000/infra/sip_sets/67xxi<br>Production release | Read/Write via FTP | mngt_ftp_67xxi | mngt_ftp_67xxi |
| /opt/a5000/infra/sip_sets/67xxi<br>Test version | Reading via FTP | ftp_67xxi | ftp_67xxi |
| /opt/a5000/infra/sip_sets/test_67xxi<br>Test version | Reading via FTP | test_connexio | test_connexio |
| /opt/a5000/infra/sip_sets/test_67xxi<br>Test version | Read/Write via FTP | mngt_test_67xxi | mngt_test_67xxi |
| /opt/a5000/infra/sip_sets/pictures<br>Pictures of 6739 SIP, 6867 SIP, 6869 SIP and 6873 SIP phones | Reading via FTP | picture | picture |
| /opt/a5000/infra/sip_sets/blustar<br>Blustar 8000i | Read/Write via FTP | blustar | blustar |

* : In the column **Dedicated directories**, the directory tree is free **but** the definition of accounts must be fully consistent with the ones defined in TMA.

In this same column, the tree is given as an example and corresponds to the one imposed for integrated TMA.

**Note : For information about how to manage pictures on 6739 SIP, 6867 SIP, 6869 SIP and 6873 SIP phones, see the document AMT/PTD/PBX/80*.**

**Note : For information on how to manage pictures on Blustar 8000i, see document AMT/PTD/TLa/0063*.**

### 11.3.2 CREATING THE ACCOUNT USED BY TERMINALS TO DEPLOY THE PRODUCTION VERSION

This account enables Mitel 6000 SIP Phones to access the deployment directory in which the terminal software and all the configuration files for the production version are located.

- Select Menu **Edit > Users > General.**
- Click **Add** to create a new user account.
- Enter the name of the account: **connexio** then click OK to confirm.
- For the **connexio** account, tick the password box and enter the associated password: **connexio**. Click OK to confirm.
- Select Menu **Edit > Users > Shared folders.**
- In the Shared folders area, click **Add** to associate the storage directory (**/opt/a5000/infra/sip_sets/deployment_67xxi)** with the **connexio** account. Tick the options used to obtain read-only rights.
- Click OK to confirm the selection. Click OK to confirm these changes.

**ATTENTION : The login and password used by Mitel 6000 SIP Phones in the production version must be "connexio".**

### 11.3.3 CREATING THE ACCOUNT USED BY TERMINALS FOR THE PRODUCTION VERSION

This account enables Mitel 6000 SIP Phones to access the storage directory in which the terminal software and all the configuration files for the production version are located.

**ATTENTION : This account must also be defined in TMA, in the FTP server configuration menu.**

- Select Menu **Edit > Users > General.**
- Click **Add** to create a new user account.
- Enter the name of the account: **ftp_67xxi** then click OK to confirm.
- For the account **ftp_67xxi**, tick the password box and enter the associated password: **ftp_67xxi**. Click OK to confirm.
- Select Menu **Edit > Users > Shared folders.**
- In the Shared folders area, click **Add** to associate the storage directory with the **ftp_67xxi** account. Tick the options used to obtain read-only rights.
- Click OK to confirm the selection. Click OK to confirm these changes.

### 11.3.4 CREATING THE ACCOUNT USED BY TERMINALS FOR THE TEST VERSION

This account enables Mitel 6000 SIP Phones to access the storage directory in which the terminal software and all the configuration files for the test version are located.



**ATTENTION : This account must also be defined in TMA, in the FTP server configuration menu.**

- Select Menu **Edit > Users > General.**
- Click **Add** to create a new user account.
- Enter the name of the account: **test_connexio** and click OK to confirm.
- For the test account, tick the password box and enter the associated password: **test_connexio**. Click OK to confirm.
- Select Menu **Edit > Users > Shared folders.**
- In the Shared folders area, click **Add** to associate the right storage directory with the **test_connexio** account. Tick the options used to obtain read-only rights.
- Click OK to confirm the selection. Click OK to confirm these changes.

### 11.3.5 CREATING THE ACCOUNT USED BY TMA (PRODUCTION VERSION)

This account enables the TMA application to place in the **Production version** directory the terminal software and configuration files for Mitel 6000 SIP Phone.



**ATTENTION : This account must also be defined in TMA, in the FTP server configuration menu.**

**For the production version** account **mngt_ftp_67xxi**

- Select Menu **Edit > Users > General.**
- Click **Add** to create a new user account.
- Enter the name of the account: **mngt_ftp_67xxi** then click OK to confirm.
- For the account **mngt_ftp_67xxi**, tick the password box and enter the associated password: **mngt_ftp_67xxi** then click OK to confirm.
- Select Menu **Edit > Users > Shared folders.**
- In the Shared folders area, click **Add** to associate the right storage directory with the **mngt_ftp_67xxi** account. Tick the options used to have read / write / delete rights.
- Click OK to confirm the selection. Click OK to confirm these changes.

### 11.3.6 CREATING THE ACCOUNT USED BY TMA (TEST VERSION)

This account enables the TMA application to place in the **Test version** directory the terminal software and configuration files for Mitel 6000 SIP Phone.



**ATTENTION : This account must also be defined in TMA, in the FTP server configuration menu.**

**For the test version** account **mngt_test_67xxi**

- Select Menu **Edit > Users > General.**
- Click **Add** to create a new user account.
- Enter the name of the account: **mngt_test_67xxi** then click OK to confirm.
- For the account **mngt_test_67xxi**, tick the password box and enter the associated password: **mngt_test_67xxi**. Click OK to confirm.
- Select Menu **Edit > Users > Shared folders.**
- In the Shared folders area, click **Add** to associate the right storage directory with the **mngt_test_67xxi** account. Tick the options used to have read / write / delete rights.
- Click OK to confirm the selection. Click OK to confirm these changes.

## 11.4 CONFIGURING AN FTP SERVER ON A PLATFORM MIVOICE 5000 SERVER FOR MITEL 6000 SIP PHONES

The mandatory prerequisite is that the FTP server manages passive mode.

**ATTENTION : TCP port 21 must be open if the MiVoice 5000 Server firewall is enabled.**

In the example below, the FTP server used is **vsftpd**. This package is installed by default when RedHat Enterprise 5 is installed on the MiVoice 5000 Server platform.

### 11.4.1 ACCOUNTS ASSOCIATED WITH THE STORAGE DIRECTORIES FOR MITEL 6000 SIP PHONES

**Tableau 11.4 :**

| DEDICATED DIRECTORIES * | RIGHT | LOGIN | PASSWORD |
|---|---|---|---|
| /opt/a5000/infra/sip_sets/deployment_67xxi<br>Production release for deployment | Reading via FTP | connexio | connexio |
| /opt/a5000/infra/sip_sets/67xxi<br>Production release | Read/Write via FTP | mngt_ftp_67xxi | mngt_ftp_67xxi |
| /opt/a5000/infra/sip_sets/67xxi<br>Test version | Reading via FTP | ftp_67xxi | ftp_67xxi |
| /opt/a5000/infra/sip_sets/test_67xxi<br>Test version | Reading via FTP | test_connexio | test_connexio |
| /opt/a5000/infra/sip_sets/test_67xxi<br>Test version | Read/Write via FTP | mngt_test_67xxi | mngt_test_67xxi |
| /opt/a5000/infra/sip_sets/pictures<br>Pictures of 6739 SIP, 6867 SIP, 6869 SIP and 6873 SIP phones | Reading via FTP | picture | picture |
| /opt/a5000/infra/sip_sets/blustar<br>Blustar 8000i | Read/Write via FTP | blustar | blustar |

* : In the Dedicated directories column, the directory tree is free but the definition of accounts must be fully consistent with the ones defined in TMA.

In this same column, the tree is given as an example and corresponds to the one imposed for integrated TMA.

**ATTENTION : As of MiVoice 5000 R5.2 SP1 on MiVoice 5000 Server, the FTP service may be installed and managed via Web Admin. In that case, the accounts used by Mitel 6000 SIP Phones are automatically defined as described in the above table at the start of the FTP service (automatic start using Ctrl I or manually via Web Admin).**
**The rights associated with these accounts, as well as their storage directory, are also automatically created as described in the next chapters.**

**Note : For information about how to manage pictures on 6739 SIP, 6867 SIP, 6869 SIP and 6873 SIP phones, see the document AMT/PTD/PBX/80*.**

**Note : For information on how to manage pictures on Blustar 8000i, see document AMT/PTD/TLa/0063*.**

### 11.4.2 CREATING THE ACCOUNT USED TO DEPLOY THE PRODUCTION VERSION ON MITEL 6000 SIP PHONES

This account has read-only rights and gives Mitel 6000 SIP Phones access to the deployment directory in which the terminal software and all the configuration files for deploying the production version are located.

- Select Menu **System > Administration > Users and groups**.
- Click **Add user**.

In the screen that opens:

- Enter the user name: **connexio**
- Enter the full name: **connexio**
- Enter the password: **connexio**
- Confirm the password: **connexio**
- Indicate the connection shell: **/bin/bash**
- Tick the box **create a personal directory** and enter it (for instance the one used for integrated TMA): **/opt/a5000/infra/sip_sets/deployment_67xxi**
- Untick the creation of a private group for the user.
- Click **Confirm** to confirm these parameters.

**ATTENTION : The login and password used by Mitel 6000 SIP Phones in the production version must be "connexio".**

### 11.4.3 CREATING THE ACCOUNT USED BY TERMINALS FOR THE PRODUCTION VERSION

This account has read-only rights and enables Mitel 6000 SIP Phones to access the storage directory in which the terminal software and all the configuration files for the production version are located.

**ATTENTION : This account must also be defined in TMA.**

- Select Menu **System > Administration > Users and groups**.
- Click **Add user**.

In the screen that opens:

- Enter the user name: **ftp_67xxi**
- Enter the full name: **ftp_67xxi**
- Enter the password: **ftp_67xxi**
- Confirm the password: **ftp_67xxi**
- Indicate the connection shell: **/bin/bash**
- Tick the box **create a personal directory** and enter it (for instance the one used for integrated TMA): **/opt/a5000/infra/sip_sets/67xxi**
- Untick the creation of a private group for the user.

- Click **Confirm** to confirm these parameters.

**ATTENTION : The login and password used by Mitel 6000 SIP Phones in the production version must be "ftp_67xxi".**

### 11.4.4 CREATING THE ACCOUNT USED BY TERMINALS FOR THE TEST VERSION

This account has read-only rights and enables Mitel 6000 SIP Phones to access the storage directory in which the terminal software and all the configuration files in test mode are located.

**ATTENTION : This account must also be defined in TMA.**

- Select Menu **System > Administration > Users and groups**.
- Click **Add user**.

In the screen that opens:

- Enter the user name: **test_connexio**
- Enter the full name: **test_connexio**
- Enter the password: **test_connexio**
- Confirm the password: **test_connexio**
- Indicate the connection shell: **/bin/bash**
- Tick the box **create a personal directory** and enter it (for instance the one used for integrated TMA): **/opt/a5000/infra/sip_sets/test_67xxi**
- Untick the creation of a private group for the user.
- Click Validate to confirm these parameters.

### 11.4.5 CREATING THE ACCOUNT USED BY TMA (PRODUCTION VERSION)

This account has read/write rights and enables the TMA application to place in the production directory the terminal software and configuration files for Mitel 6000 SIP Phones.

**ATTENTION : This account must also be defined in TMA.**

**For the production version**

- Select Menu **System > Administration > Users and groups**.
- Click **Add user**.

In the screen that opens:

- Enter the user name: **mngt_ftp_67xxi**
- Enter the full name: **mngt_ftp_67xxi**
- Enter the password: **mngt_ftp_67xxi**
- Confirm the password: **mngt_ftp_67xxi**
- Indicate the connection shell: **/bin/bash**
- Tick the box **create a personal directory** and enter it (for instance the one used for integrated TMA): **/opt/a5000/infra/sip_sets/67xxi**
- Untick the creation of a private group for the user.

- Click Validate to confirm these parameters.

### 11.4.6 CREATING THE ACCOUNT USED BY TMA (TEST VERSION)

This account has read/write rights and enables the TMA application to place in the test directory the terminal software and configuration files for Mitel 6000 SIP Phones.



**ATTENTION : This account must also be defined in TMA.**

**For the test version**

- Select Menu **System > Administration > Users and groups**.
- Click **Add user**.

In the screen that opens:

- Enter the user name: **mngt_test_67xxi**
- Enter the full name: **mngt_test_67xxi**
- Enter the password: **mngt_test_67xxi**
- Confirm the password: **mngt_test_67xxi**
- Indicate the connection shell: **/bin/bash**
- Tick the box **create a personal directory** and enter it (for instance the one used for integrated TMA): **/opt/a5000/infra/sip_sets/test_67xxi**
- Untick the creation of a private group for the user.
- Click Validate to confirm these parameters.

### 11.4.7 CREATING THE MNGT_FTP_67XXI GROUP

This group has read / write rights and is used to assign the appropriate rights to the **ftp_67xxi** and **mngt_ftp_67xxi** account.

- Select Menu **System > Administration > Users and groups**.
- Click **Add group**.
- Enter the name of the group: **mngt_ftp_67xxi**
- Click Validate to confirm these parameters.

### 11.4.8 CREATING THE MNGT_TEST_67XXI GROUP

This group has read / write rights and is used to assign the appropriate rights to the **test_connexio** and **mngt_test_67xxi** account.

- Select Menu **System > Administration > Users and groups**.
- Click **Add group**.
- Enter the name of the group: **mngt_test_67xxi**
- Click Validate to confirm these parameters.

### 11.4.9 CHANGE THE OWNER AND GROUP ASSOCIATED WITH THE MITEL 6700 SIP PHONE DIRECTORY.

Open a terminal window then go to **/opt/a5000/infra/sip_sets** (using the example used from the integrated TMA).

- Type in the following command:

  **chown ftp_67xxi:mngt_ftp_67xxi 67xxi**



**ATTENTION : Respect he space before the last Mitel 6700 SIP Phone.**

### 11.4.10 MODIFY THE RIGHTS ASSOCIATED WITH THE MITEL 6700 SIP PHONE DIRECTORY.

Open a terminal window then go to **/opt/a5000/infra/sip_sets** (using the example used from the integrated TMA).

- Type in the following command:

  **chmod 577 67xxi**

### 11.4.11 CHANGE THE OWNER AND GROUP ASSOCIATED WITH THE TEST FOLDER.

Open a terminal window then go to **/opt/a5000/infra/sip_sets** (using the example used from the integrated TMA).

- Type in the following command:

  **chown test_connexio:mngt_test_67xxi test_67xxi**



**ATTENTION : Respect the space before the last test_67xxi.**

### 11.4.12 CHANGE THE RIGHTS ASSOCIATED WITH THE TEST DIRECTORY.

Open a terminal window then go to **/opt/a5000/infra/sip_sets** (using the example used from the integrated TMA).

- Type in the following command:

  **chmod 577 test_67xxi**

### 11.4.13 MODIFY THE FILE VSFTPD.CONF UNDER /ETC/VSFTPD.

The modifications consist in:

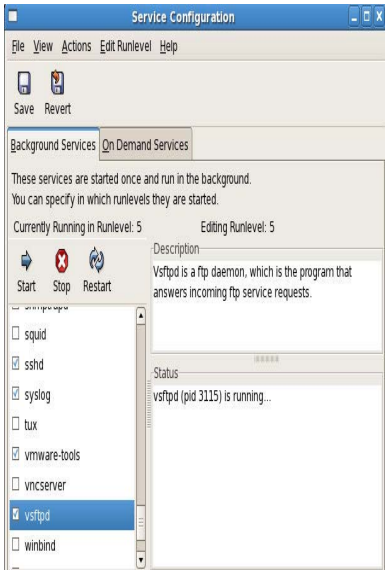
- disallowing anonymous connections: you must connect to the FTP server with a user or system account (**anonymous_enable=NO)**.
- Limit the number of simultaneous connections to 1000 (**max_clients = 1000)**.

These modifications appear in bold in the detailed file used as in Chapter 11.2.12.

- Then start the **vsftpd** service.

Select Menu **System > Administration > Server parameters > Services.**

Select the **vsftps** service and click **Start**.



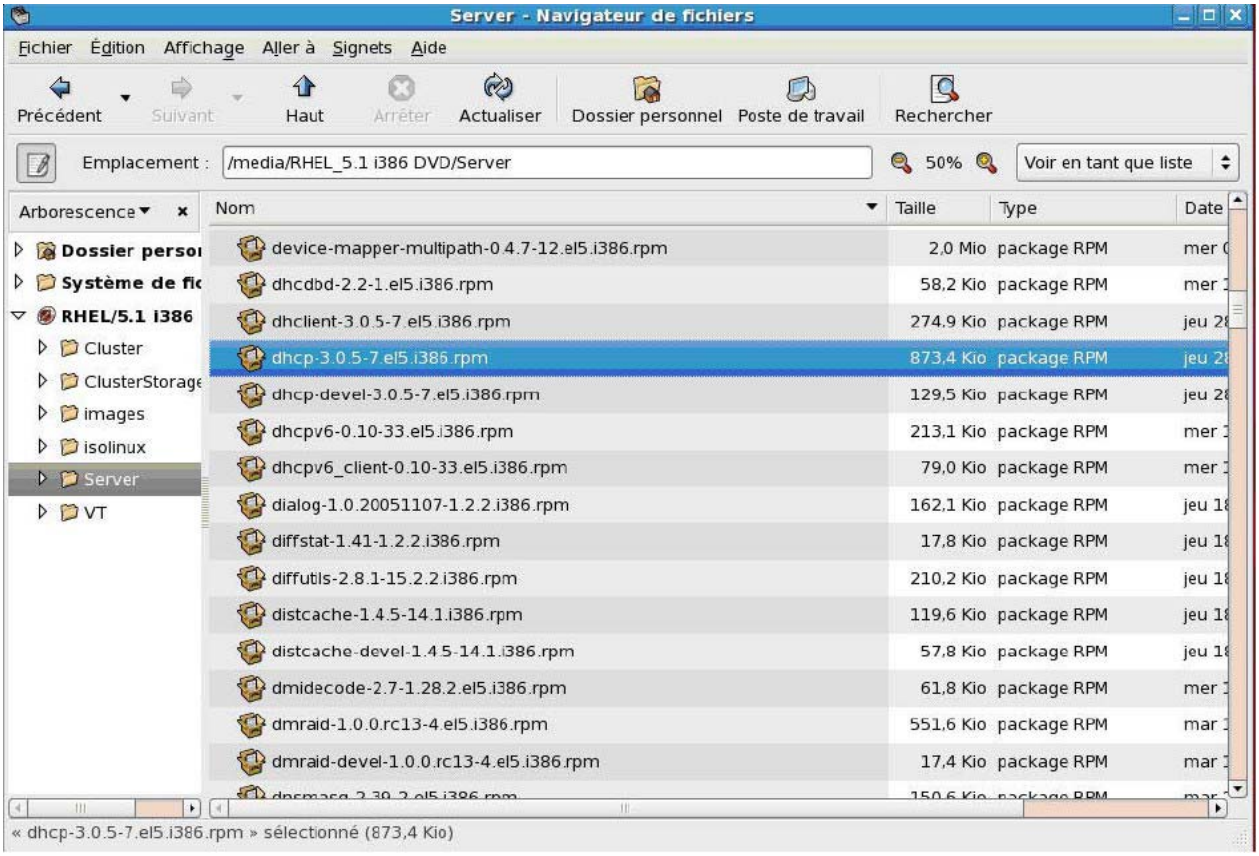
# 12 APPENDIX 1

## 12.1 INSTALLING DHCP PACKAGING IN LINUX REDHAT 5

- Insert the Linux RedHat5 installation DVD-ROM.
- Right-click the CD/DVD drive icon and increase the volume.




- Go to the DVD directory: /Server




- Start the execution of the " dhcp-x.x.x-x..i386.rpm " package and install it.

# 13 APPENDIX 2

## 13.1 LIST AND MEANING OF THE STANDARD NETWORK PARAMETERS USED BY THE DHCP SERVER INTEGRATED INTO MITEL 5000 GATEWAYS AND MIVOICE 5000 SERVER

- **DNS update style**

  This parameter enables the DHCP server to update the DNS inputs, especially if a server's IP address changes. The two (**ad-hoc** and **interim**) modes describe the methods of carrying out these updates. Today, it is advisable not to use ad-hoc style. By default, this parameter is set to **none** (no DNS server update by the integrated DHCP server).

- **The network is authoritative**.

  If the DHCP server is authoritative, this implies that the configuration information on a given network segment is correct and authoritative. Moreover, if the client asks for an IP address on a network segment that the server knows to be invalid for this segment, the server will respond with a DHCPNAK message, resulting at the client's in the abandonment of its IP address and the request for a new one.

- **Ignore**

  ignore **bootp**: do not respond to BOOTP messages

  ignore **declines**: do not respond to DHCPDECLINE messages indicating a network clash.

  ignore **booting**: do not allow the client to obtain an IP address. Declaration valid in a host declaration only

  By default, if these parameters are not entered (checkbox not ticked), these options are authorised.

- **dynamic bootp**

  Dynamic-bootp is used to indicate that the DHCP must respond to BOOTP requests by giving the address of this range. Not used by default.

- **Subnet-mask option**

  The subnet-mask option specifies the terminal's subnet mask as defined in RFC 950 (RFC = Request For Comments). If no subnet-mask option is provided within the block range, dhcpd will use as, a last resort, the declaration of subnet to which the address being assigned belongs. However, any subnet-mask option declaration will replace the subnet mask specified in the subnet declaration.

- **Allow**

  As of R6.2, this parameter is used to indicate whether only **known clients** are managed by the integrated DHCP server or whether **all clients** are managed by the integrated DHCP server.

  **Known clients** have a defined Vendor Class with some associated parameters. New devices can be managed via the Template management menu. These new devices must be associated with a new Vendor Class.

  If the integrated DHCP server must also respond to requests from devices without Vendor Class (servers, PC, etc.) set the Allow parameter to **All clients**.

  allow **known clients**: allows IP addresses to be assigned to clients known to the pool (clients which have a host declaration with an associated Vendor Class).

  allow **unknown clients**: allows IP addresses to be assigned to clients not known to the pool (clients which do not have any host declaration).

  allow **dynamic bootp clients:** allows responses to BOOTP requests in the pool.

  allow **authenticated clients:** allows an IP address to be assigned to a client which has been authenticated in the pool using the DHCP authentication protocol (not available at the moment).

allow **all clients:** allows the an IP address to be assigned to all the clients in the pool, especially those without Vendor Class.

By default, if these parameters are not entered (checkbox not ticked), IP addresses may be assigned to clients not known to the pool (clients which do not have any host declaration).

- **NTP server address** (ntp-servers option;)

  This option is used to define the IP address of an NTP server (RFC 1035) available on the terminal.

- **Domain name** (domain name option)

  This option specifies the domain name which the terminal must use while resolving some host names via the DNS name server.

- **Domain server address** (domain name server option)

  The domain name server option indicates the IP address of a domain name server (DNS: Domain Name System) (STD 13, RFC 1035) available for the terminals. The DNS is a system used to determine a correspondence between an IP address and a domain name and, more generally, to find information from a domain name. Resolving a domain name implies finding the associated IP address.

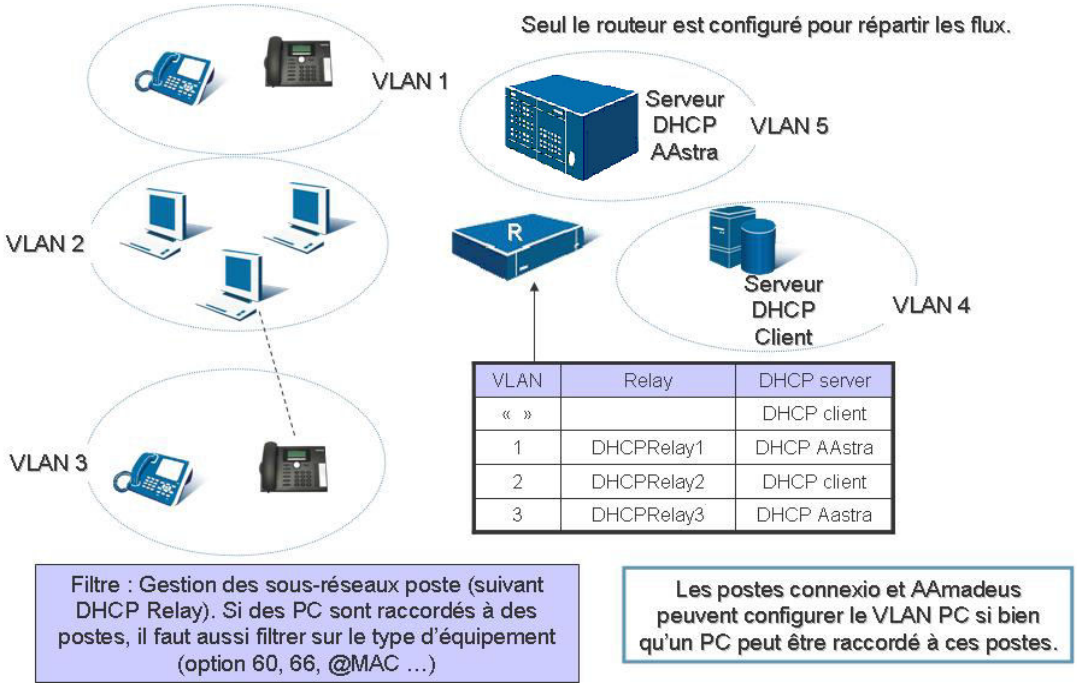
- **Broadcast address**

  This option specifies the broadcast address to use for the subnet in question. The legal values are specified in Section 3.2.1.3 of STD 3 (RFC 1122).

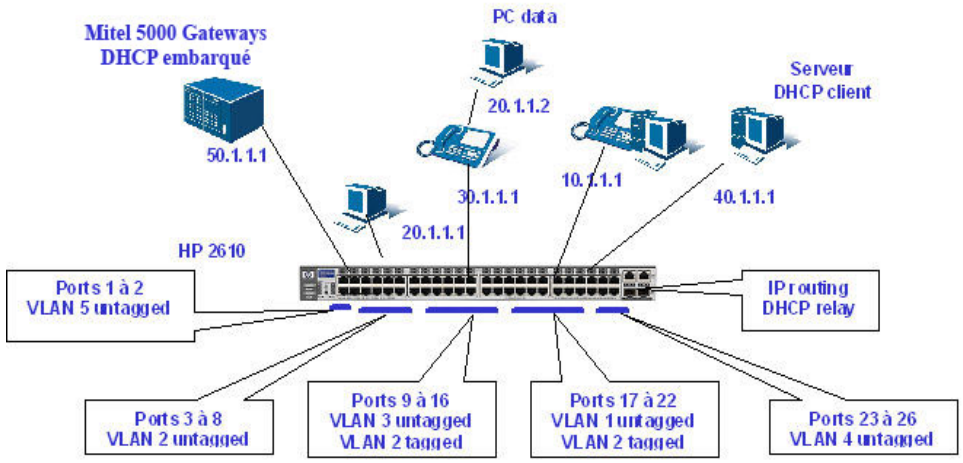
# 14 APPENDIX 3

## 14.1 EXAMPLES OF ARCHITECTURES ASSOCIATED WITH THE DHCP SERVER INTEGRATED INTO MITEL 5000 GATEWAYS

## 14.2 THE DEVICES ARE INSTALLED ON DIFFERENT SUBNETS AND THE CLIENT ALREADY HAS A DHCP SERVER:




In this example, the client already has a DHCP server he is using to manage his network devices (PC, servers, etc.). The objective is to manage the Mitel devices via the DHCP server integrated into Mitel 5000 Gateways without modifying the client's DHCP server configuration.




Configuring the DHCP relay agent:

- VLAN 1,3 to Mitel DHCP server
- VLAN 2 to DHCP client

Example of Level 3 switch configuration:

```
Startup configuration:
; J4900B Configuration Editor; Created on release #H.10.38
hostname "ProCurve Switch 2626"
ip routing
snmp-server community "public" Unrestricted
vlan 1
        name "VLAN 1"
        untagged 17-22
        ip address 10.1.1.254 255.255.255.0
        ip helper-address 50.1.1.1
        no untagged 1-16,23-26
        exit
vlan 5
        name "DHCP emb"
        untagged 1-2
        ip address 50.1.1.254 255.255.255.0
        exit
vlan 2
        name "VLAN 2"
        untagged 3-8
        ip address 20.1.1.254 255.255.255.0
        ip helper-address 40.1.1.1
        tagged 9-22
        exit
vlan 4
        name "DHCP client"
        untagged 23-26
        ip address 40.1.1.254 255.255.255.0
        exit
vlan 3
        name "VLAN 3"
        untagged 9-16
        ip address 30.1.1.254 255.255.255.0
        ip helper-address 50.1.1.1
        exit
primary-vlan 2
```

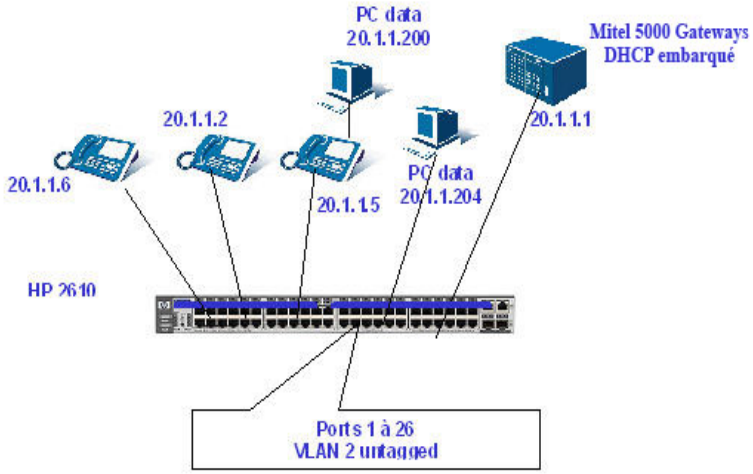
Impact on the client network:

Configuring the router to manage an a subnet-based DHCP relay agent and modifying the switch ports configuration to assign them the right VLAN.



**ATTENTION : This configuration does not allow the management of a terminal i7xx with associated PC in full DHCP mode. A PC can be connected directly to the ports of the switch where a Mitel terminal is normally connected.**

### 14.2.1 ONLY ONE DHCP SERVER. ALL THE NETWORK DEVICES, INCLUDING THE INTEGRATED DHCP SERVER, ARE INSTALLED ON THE SAME IP NETWORK:




In this example, the client does not have anyDHCP server to manage his own network devices (PC, servers, etc.). The objective is to manage the Mitel devices via the DHCP server integrated into Mitel 5000 Gateways.

**ATTENTION : It can be implemented on configurations containing a few terminals and a few network devices since there is no specific VLAN for the phones.**

Impact on the client network: None

Example of Level 3 switch configuration:
Startup configuration:
; J4900B Configuration Editor; Created on release #H.10.38
hostname "ProCurve Switch 2626"
ip routing
snmp-server community "public" Unrestricted
vlan 2
    name "VLAN 2"
    untagged 1-26
    ip address 20.1.1.254 255.255.255.0
    exit
primary-vlan 2

# 15 APPENDIX 4: MANAGING THE TERMINALS MANUALLY MIVOICE 5300 IP PHONE AND MITEL 6000 SIP PHONE

## 15.1 CONFIGURING AN FTP SERVER ON A PLATFORM WINDOWS 2000/ 2003 FOR MIVOICE 5300 IP PHONES

This type of configuration must be used to manually manage the software and configuration files of MiVoice 5300 IP Phones (**TMA not used**).

**ATTENTION : Mitel strongly discourages the use of this operating mode.**

The mandatory prerequisite is that the FTP server manages passive mode.

In the example below, the FTP server used is Filezilla Server.

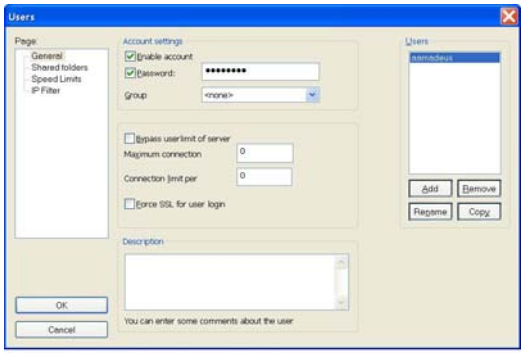
After installing the FTP server, select the menu **Edit > Users > General**.

Click **Add** to create a new user account.

Enter the account name: aamadeus and click OK to confirm.

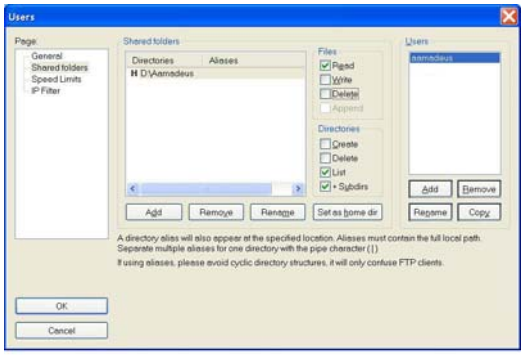
For the aamadeus account, tick the password box and enter the associated password: aamadeus

Click OK to confirm.



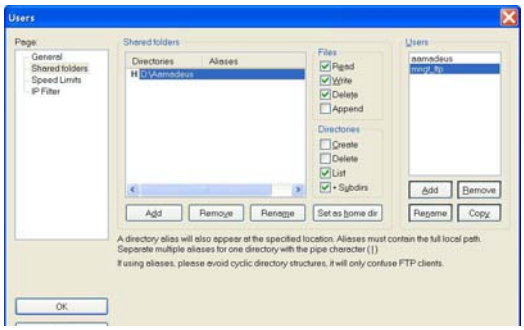

Select Menu **Edit  Users  Shared foldersEdit > Users > Shared folders**.

In the shared folder area, click **Add** to assign the aamadeus user account a storage directory in which the firmware and all the MiVoice 5300 IP Phone configuration files will be made available.




Click OK to confirm the selection. Click OK to confirm these changes.

This account enables MiVoice 5300 IP Phones to download their firmware and configuration files. For configuration file management, create another account and then modify the rights associated with this account to authorise the writing and deletion of files on the storage directory which will be identical to the one used by the aamadeus account.




## 15.2 CONFIGURING AN FTP SERVER ON A PLATFORM MIVOICE 5000 SERVER FOR MIVOICE 5300 IP PHONES

This type of configuration must be used to manually manage the software and configuration files of MiVoice 5300 IP Phones.

The mandatory prerequisite is that the FTP server manages passive mode.

**ATTENTION : TCP port 21 must be open if the MiVoice 5000 Server firewall is enabled.**

In the example below, the FTP server used is vsftpd. This package is installed by default when RedHat Enterprise 5 is installed on the MiVoice 5000 Server platform.

Proceed as follows:

### 1. Create the mngt_ftp account.

This account has read / write rights and is used to fully manage the configuration files left on the aamadeus account.

- Select Menu **System > Administration > Users and groups**.
- Click **Add user**.
- The following menu is displayed:




- Enter the user name: mngt_ftp
- Enter the full name: mngt_ftp
- Enter the password: mngt_ftp
- Confirm the password: mngt_ftp

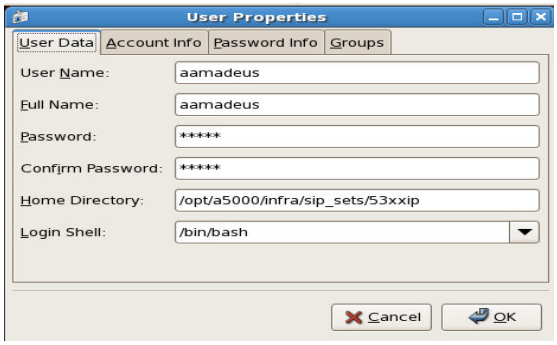
- Indicate the connection shell: /bin/bash
- Tick the box **create private directory** and enter the following: /opt/a5000/infra/sip_sets
- Untick the creation of a private group for the user.
- Click Validate to confirm these parameters.

### 2. Creating the aamadeus account

This account has read rights only and is used by MiVoice 5300 IP Phones only.

- Select Menu **System > Administration > Users and groups**.
- Click **Add user**.

The following menu is displayed:




- Enter the user name: aamadeus
- Enter the full name: aamadeus
- Enter the password: aamadeus
- Confirm the password: aamadeus
- Indicate the connection shell: /bin/bash
- Tick the box **create private directory** and enter the following: /opt/a5000/infra/sip_sets/53xxip
- Untick the creation of a private group for the user.
- Click Validate to confirm these parameters.

### 3. Create the mngt_ftp group.

This group has read / write rights and is used to assign the appropriate rights to the aamadeus and mngt_ftp account.

- Select Menu **System > Administration > Users and groups**.
- Click **Add group**.
- Enter the group name: mngt_ftp
- Click Validate to confirm these parameters.

### 4. Change the owner and group associated with the aamadeus account.

- Open a terminal window then go to /opt/a5000/infra/sip_sets.
- Type in the command:

chown -R aamadeus:mngt_ftp 53xxip

### 5. Change the rights associated with the aamadeus account.

- Open a terminal window then go to /opt/a5000/infra/sip_sets.
- Type in the command:

chmod -R 577 53xxip

### 6. Modify the file vsftpd.conf under /etc/vsftpd.

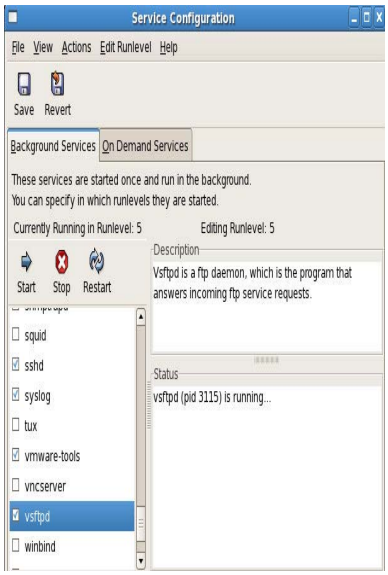
The modifications consist in:

- disallowing anonymous connections: you must connect to the FTP server with a user or system account (**anonymous_enable=NO**).
- Limit the number of simultaneous connections to 1000 (**max_clients = 1000**).

These modifications appear in bold in the detailed file used as in Chapter 11.2.12.

### 7. Starting the vsftpd service.

- Select Menu System > Administration > Server parameters > Services.
- Select the vsftps service and click Start.




**ATTENTION : After upgrading the system software, the access rights for the mngt_ftp and aamadeus accounts must be redefined, as well as the owner and group associated with these accounts.**

## 15.3 CONFIGURING AN FTP SERVER ON A WINDOWS 2000/2003 PLATFORM FOR MITEL 6000 SIP PHONES

This type of configuration must be used to manually manage the software and configuration files of Mitel 6000 SIP Phones (**TMA not used**).

**ATTENTION : Mitel strongly discourages the use of this operating mode.**

The procedure is the same for MiVoice 5300 IP Phones using the account **connexio** and the password **connexio**.

## 15.4 CONFIGURING AN FTP SERVER ON A MIVOICE 5000 SERVER PLATFORM FOR MITEL 6000 SIP PHONES

This type of configuration must be used to manually manage the software and configuration files of Mitel 6000 SIP Phones.

The mandatory prerequisite is that the FTP server manages passive mode.

**ATTENTION : TCP port 21 must be open if the MiVoice 5000 Server firewall is enabled.**

In the example below, the FTP server used is vsftpd. This package is installed by default when RedHat Enterprise 5 is installed on MiVoice 5000 Server.

Proceed as follows:

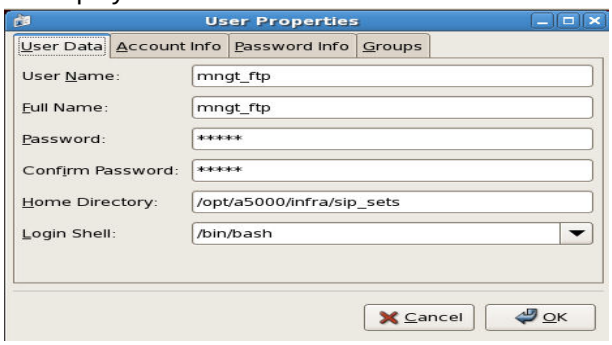
**1. Create the mngt_ftp account.**

This account has read / write rights and is used to fully manage the configuration files left on the connection account.

Select Menu **System > Administration > Users and groups**.

Click **Add user**.

The following menu is displayed:




Enter the user name: mngt_ftp

Enter the full name: mngt_ftp

Enter the password: mngt_ftp

Confirm the password: mngt_ftp

Indicate the connection shell: /bin/bash

Tick the box “create private directory” and enter the following: /opt/a5000/infra/sip_sets

Untick the creation of a private group for the user.

Click Validate to confirm these parameters.

### 2. Creating the connexio account

This account has read rights only and is used by Mitel 6000 SIP Phones only.

Select Menu **System > Administration > Users and groups**.

Click **Add user**.

The following menu is displayed:




Enter the user name: connexio

Enter the full name: connexio

Enter the password: connexio

Confirm the password: connexio

Indicate the connection shell: /bin/bash

Tick the box **create private directory** and enter the following: /opt/a5000/infra/sip_sets/67xxi

Untick the creation of a private group for the user.

Click Validate to confirm these parameters.

### 3. Create the mngt_ftp group.

This group has read / write rights only and is used to assign the appropriate rights to the connection and mngt_ftp account.

Select Menu **System > Administration > Users and groups**.

Click **Add group**.

Enter the group name: mngt_ftp

Click Validate to confirm these parameters.

### 4. Change the owner and group associated with the connexio account.

Open a terminal window then go to /opt/a5000/infra/sip_sets.

Type in the command:

chown -R connexio:mngt_ftp 67xxi

### 5. Change the rights associated with the connexio account.

Open a terminal window then go to /opt/a5000/infra/sip_sets.

Type in the command:

chmod -R 577 67xxi

### 6. Modify the file vsftpd.conf under /etc/vsftpd.

The modifications consist in:

- disallowing anonymous connections: you must connect to the FTP server with a user or system account (**anonymous_enable=NO)**.
- Limit the number of simultaneous connections to 1000 (**max_clients = 1000)**.

These modifications appear in bold in the detailed file used as in Chapter 11.2.12.

### 7. Starting the vsftpd service.

Select Menu **System > Administration > Server parameters > Services.**

Select the vsftps service and click Start.




**ATTENTION : After upgrading the system software, the access rights for the mngt_ftp and aamadeus accounts must be redefined, as well as the owner and group associated with these accounts.**

# 16 APPENDIX 5: CONFIGURING MIVOICE 5300 IP PHONES MANUALLY

Manual configuration of MiVoice 5300 IP Phones may be envisaged for implementing some terminals on a single-site Mitel 5000 Gateways system for which the integrated TMA is not used. This solution requires the availability of an integrated or external FTP server. The network parameters required by the terminal to work well are declared manually, either from the terminal or from the WEB interface.

These network parameters can also be configured and downloaded from the FTP server.

In this case, the IP address of the FTP server is the only network parameter that requires manual configuration. Configuration files are made available manually on the FTP server storage area by the administrator using the right account.

The firmware compatible with the MiVoice 5000 solution, as well as the MiVoice 5300 IP Phone initialisation file (tm.config.<TT>.<VN>.ftp), must be downloaded to the terminal.

## 16.1 DEFAULT CONFIGURATION WHEN THE TERMINAL IS INSTALLED FOR THE FIRST TIME

A new terminal has the following factory configuration (default configuration):

- The **DHCP** option is enabled.
- The terminal's default IP address is: 192.168.104.33
- The default sub-net mask value is: 255.255.255.0
- The **Software download mode** option is in auto mode.
- The **Data download mode** option is enabled.



**ATTENTION : Its default firmware is compatible with R5000.1 R5.1A. It must be updated if the release provided with the system is more recent.**

## 16.2 MANUAL CONFIGURATION FROM MIVOICE 5300 IP PHONES

Power on the terminal without connecting it to the LAN, or by connecting a PC directly via a twisted network cable to the terminal LAN.

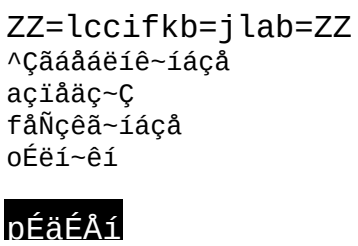
The following message is displayed on the terminal.

DHCP failed

No response from DHCP

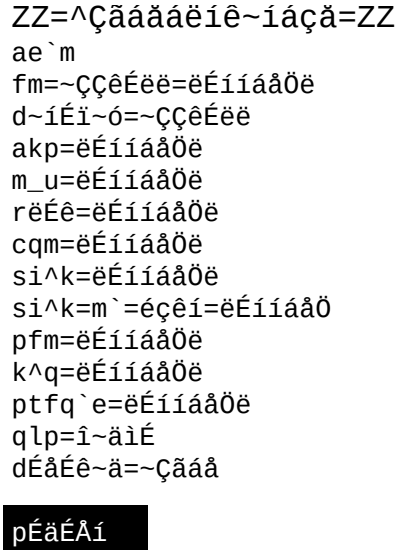
Press the interactive key **OK**:

The screen displays the following:



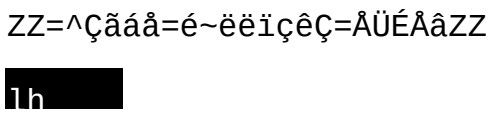

Go to the **Administration** input and press the fox key **Select**.

The following screen is displayed:



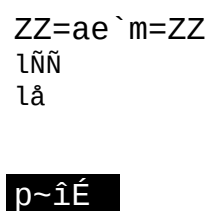

Go to the **DHCP** input and press the fox key **Select**.

The following screen is displayed:



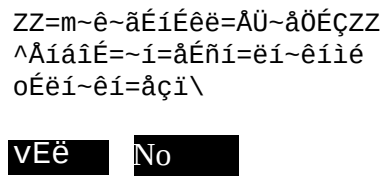
Enter the default password (**0000**) and press the fox key **OK**.

The following screen is displayed:




Select **Off** then press the fox key **Save**.

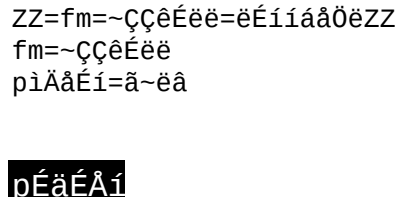
The following screen is displayed:




Press the fox key “No”.

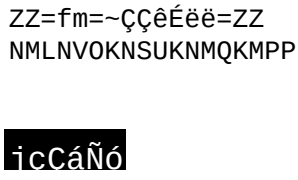
Go to the **IP address settings** input and press the fox key **Select**.

The following screen is displayed:




Select **IP address** then press the fox key **Select**.

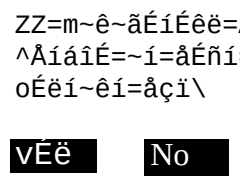
The following screen is displayed:




Press the fox key **Modify**.

Enter the terminal IP address using the numeric keypad, and back it up by pressing the fox key **Save** (use the key **C** to correct any incorrect entry).

The following screen is displayed:

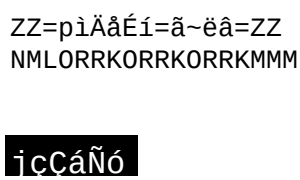


Press the fox key “No”.

Press C to return to the previous menu.

Select Subnet mask then press the fox key Select.

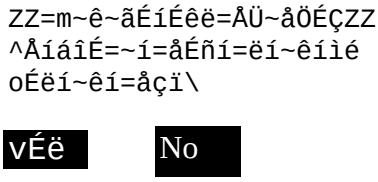
The following screen is displayed:




Press the fox key **Modify**.

Enter the terminal subnet mask using the numeric keypad, and back it up by pressing the fox key **Save** (use the key **C** to correct any incorrect entry).

The following screen is displayed:

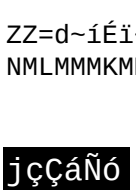



Press the fox key **No**.

Press **C** twice to return to the Administration menu.

Go to the **Gateway address** input and press the fox key **Select**.

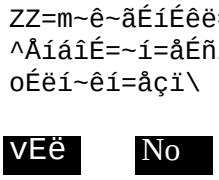
The following screen is displayed:




Press the fox key **Modify**.

Enter the network gateway address (router) used by the terminal, with the numeric keypad, and back it up by pressing the fox key **Save** (use the key **C** to correct any incorrect entry).

The following screen is displayed:

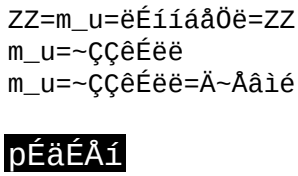


Press the fox key **No**.

Press **C** to return to the previous menu.

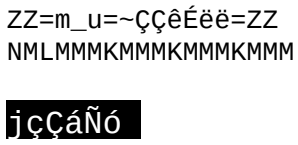
Select **PBX settings** then press the fox key **Select**.

The following screen is displayed:




Select **PBX address** then press the fox key **Select**.

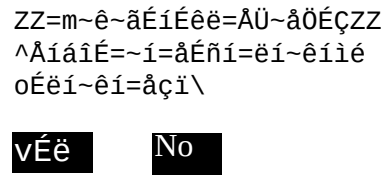
The following screen is displayed:




Press the fox key **Modify**. Enter the SIP access point address used by the terminal, with the numeric keypad, and back it up by pressing the fox key **Save** (use the key **C** to correct any incorrect entry).

***The DNS_NAME field must be deleted so as to enter an IP address (DNS settings section).***

The following screen is displayed:

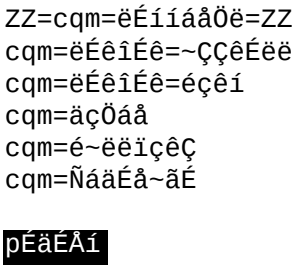



Press the fox key **No**.

Press **C** to return to the previous menu.

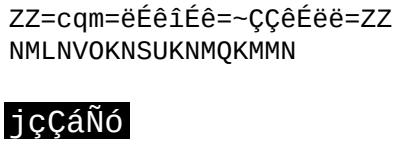
Select **FTP settings** then press the fox key **Select**.

The following screen is displayed:




Select **FTP server address** then press the fox key **Select**.

The following screen is displayed:




Press the fox key **Modify**.

Enter the FTP server address using the numeric keypad, and back it up by pressing the fox key **Save** (use the key **C** to correct any incorrect entry).

***Manual entry of FTP server address has priority over a negotiation with the DHCP server via option 66.***

The following screen is displayed:

```
ZZ=m~ê~ãÉíÉêë=ÅÜ~åÖÉÇZZ
^ÅíáîÉ=~í=åÉñí=ëí~êíìé
oÉëí~êí=åçï\

vÉë      No
```

Press the fox key **No**.

Press **C** to return to the previous menu.

Select **FTP filename** then press the fox key **Select**.

The following screen is displayed:

```
ZZ=cqm=ÑáäÉå~ãÉ=ZZ
~~ãñáé|îGKÑíé

jçÇáÑó
```

Check that the name of the firmware corresponds to:**aamxip_v*.ftp**

Press the left arrow on the navigation key to return to the previous menu.

Select **VLAN settings** then press the fox key **Select**.

The following screen is displayed:

```
ZZ=si^k=ëÉííáåÖë=ZZ
si^k
si^k=ìëÉê=éêáçêáíó
si^k=fa

pÉäÉÅí
```

Select **VLAN** then press the fox key **Select**.

The following screen is displayed:

```
ZZ=si^k=ZZ
lÑÑ
lå

p~îÉ
```

Select **On** then press the fox key **Save**.

The following screen is displayed:

```
ZZ=m~ê~ãÉíÉêë=ÅÜ~åÖÉÇZZ
^ÅíáîÉ=~í=åÉñí=ëí~êíìé
oÉëí~êí=åçï\

vÉë      No
```

Press the fox key **No**.

Select **VLAN user priority** then press the fox key **Select**.

The following screen is displayed:

```
ZZ=si^k=ìëÉê=éêáçêáíó=ZZ
mêáçêáíó=M
mêáçêáíó=N
mêáçêáíó=O
K

jçÇáÑó
```

Press the fox key **Modify** then select the priority value associated with the terminal VLAN (by default, 6). Confirm by pressing the fox key **Save**

The following screen is displayed:

```
ZZ=m~ê~ãÉíÉêë=ÅÜ~åÖÉÇZZ
^ÅíáîÉ=~í=åÉÑí=ëí~êíìé
oÉëí~êí=åçï\

vÉë      No
```

Press the fox key **No**.

Press **C** to return to the previous menu.

Select **VLAN ID** then press the fox key **Select**.

The following screen is displayed:

```
ZZ=si^k=faEMKKQMVQF=ZZ
NMLM

jçÇáÑó
```

Press the fox key **Modify** and enter the terminal's VLAN number. Confirm by pressing the fox key **Save**

The following screen is displayed:

```
ZZ=m~ê~ãÉíÉêë=ÅÜ~åÖÉÇZZ
^ÅíáîÉ=~í=åÉÑí=ëí~êíìé
oÉëí~êí=åçï\

vÉë      No
```

Press the fox key **No**.

Press **C** twice to return to the previous menu.

Select **SIP settings** then press the fox key **Select**.

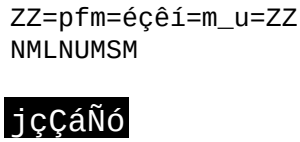
The following screen is displayed:

```
ZZ=pfm=ëÉííáåÖë=ZZ
pfm=éçêí=m_u
pfm=éçêí=m_u=Ä~Åâìé
pfm=éçêí=éÜçåÉ

pÉäÉÅí
```

Select **SIP port PBX** then press the fox key **Select**.

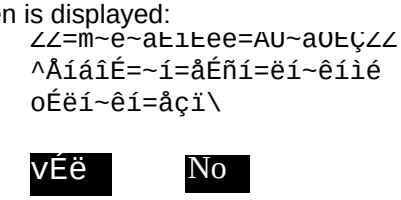
The following screen is displayed:




Press the fox key **Modify** and enter the SIP PBX port number (5060 by default). Confirm by pressing the fox key **Save**.

***UDP ports 5060 (signal flow) and 30000 (voice flow) must be open on the MiVoice 5000 Server if the firewall is enabled.***

The following screen is displayed:

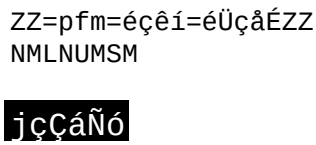



Press the fox key **No**.

Press **C** to return to the previous menu.

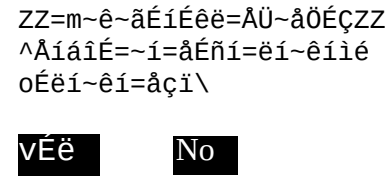
Select **SIP port phone** then press the fox key **Select**.

The following screen is displayed:




Press the fox key **Modify** and enter the SIP terminal port number (5060 by default). Confirm by pressing the fox key **Save**

The following screen is displayed:

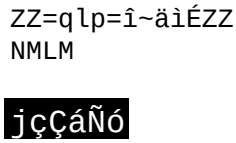



Press the fox key **No**.

Press **C** twice to return to the Administration menu.

Select **TOS value** then press the fox key **Select**.

The following screen is displayed:

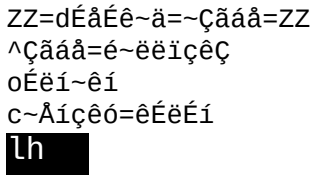



Press the fox key **Modify** and enter the value in decimal of the TOS field (184, by default). Confirm by pressing the fox key **Save**

Press **C** to return to the Administration menu.

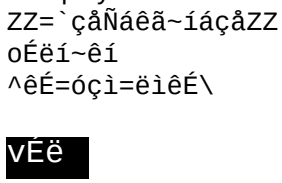
Select **General admin** then press the fox key **Select**.

The following screen is displayed:




Select **Restart** then press the fox key **OK**.

The following screen is displayed:




Press the fox key **Yes** to confirm terminal restart.

## 16.3 MANUAL CONFIGURATION FROM THE WEB INTERFACE

Prerequisites: The terminal or PC network parameters are configured to set up terminal/web user interface connection.

- Enter the terminal IP address in the web browser window in http mode (http:// ...),
- Select **Configuration Page**.
- Enter the username and password.

  Default value:

  - Username: admin
  - Password: 10/0000

These values can be modified in the **Miscellaneous** tab. See the corresponding section.

The main screen is displayed.



**Note : The FTP server and FTP file lines give the current values of the FTP server IP address and the name of the firmware to be downloaded, as well as the origin of these values:**

- **Manual entry or option negotiated via the configuration files**
- **Options 66 and 67 negotiated with the DHCP server**
- **Bootp nextserver and filename option negotiated with the DHCP server.**

- Select the **Network** tab to access the network configuration.
- Set the **DHCP_ENABLED** field to **Off**.
- Fill in the fields corresponding to the terminal IP address, subnet mask and gateway (router) IP address.
- Confirm by pressing **Save Settings.**

**Declaring the SIP gateway used by MiVoice 5300 IP Phone**

To set up communication with the SIP gateway, the system address must be entered in the terminal's web configuration interface.

Procedure:

- Click the **PBX** tab.

  Fill in the following columns:

  - PBX ADDRESS: IP address of the UCV card on a Mitel 5000 Gateways system, or of the MiVoice 5000 Server network card.



**Note : The DNS_NAME field must be deleted so as to enter an IP address.**

  - SIP_PORT_PBX: **10/5060**
  - SIP_PORT_PHONE: **10/5060**
  - USER_PHONE_NUMBER (the same as declaring a subscription on the system management portal)
  - DNS_NAME: delete the content of the field.

The other pre-completed or uncompleted columns are optional.

Confirm by pressing **Save Settings**.

### Declaring the FTP server

- Select the **Download**tab.

The terminals' firmware release and configuration files are made available, by default, in the FTP server storage directory integrated into the system's UCV card.

The first time the terminal connects to the FTP server, these files are automatically transferred to the terminal in order to update the terminal firmware and initialisation file (TM file).

- SW_DNLD_MODE: check that this field is set to AUTO mode.
- DA_DNLD_MODE: check that this field is set to ON
- FTP_SERVER: enter the FTP server address.
- FTP_FILENAME: check the name of the terminal firmware to download from the FTP server (**aamxip_v*.ftp**).

The character **v*** indicates that the most recent version of the terminal firmware has to be downloaded. The FTP server included in the system UCV may have two terminal versions.

Confirm by pressing **Save Settings**.

**ATTENTION : Manual entry of FTP server address has priority over a negotiation with the DHCP server via option 66.**

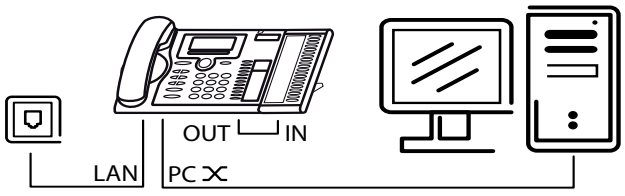
### Additional configurations (VLAN and QoS)

The IP telephony network part is generally associated with a particular VLAN, separated from the actual "computer or data" network in the company.

The VLAN tab is used to specify the corresponding terminal VLAN characteristics.

Contact the network administrator to obtain the values to declare on this page.

The terminal also connects the PC to the network via the PC X socket located at the back of the terminal; this tab is equally used to configure the PC port in question (see figure below). In a configuration with associated PC, the terminal must be connected to a port of the switch belonging to the two VLANs (ToIP and data).




- Click the **VLAN** tab.
- Fill in the fields concerning the terminal's VLAN:
  - VLAN_ENABLED (by default, VLAN is disabled (VLAN_ENABLED: Off)
  - VLAN_PRIO
  - VLAN_ID
- Fill in the VLAN fields of the PC connected to the terminal (if necessary):
  - VLANPC_ENABLED (by default, VLANPC is disabled (VLANPC_ENABLED: Off)
  - VLANPC_TAGS
  - VLANPC_PRIO
  - VLAN_ID

Confirm by pressing **Save Settings**.

**Quality of Service (QoS)**

- Select the **Miscellaneous** tab.

Contact the network administrator to obtain the values to declare on this page.

- Confirm by pressing **Save Settings**.

**Changing the password for access to the terminal configuration interface**

- Select the **Miscellaneous** tab.
- In the ADMIN_PASSWORD field, enter the new password.
- Confirm by pressing **Save Settings**.
- Restart the terminal using the Restart menu, to take account of the configuration update.
- Check the configuration by clicking the **Status** tab.

### 16.3.1 MODES SUPPORTED BY THE TERMINAL'S INTEGRATED SWITCH PORTS

The LAN and PC ports of MiVoice 5300 IP Phones support the following three transmission modes:

- Auto-negotiation
- Half-duplex (10Mb/s or 100 Mb/s)
- Full-duplex (10Mb/s or 100 Mb/s)

The PC port may also be disabled: value set to Off.

**Displaying the current configuration on the terminal:**

Press the terminal's **C** key for a few seconds:

The screen displays the following:

```
ZZ=lccifkb=jlab=ZZ
^Çãáåáëíê~íáçå
açïåäç~Ç
fåÑçêã~íáçå
oÉëí~êí

pÉäÉÅí
```

Go to the **Administration** input and press the fox key **Select**.

The following screen is displayed:

```
ZZ=^Çãáåáëíê~íáçå=ZZ
ae`m
fm=~ÇÇêÉëë=ëÉííáåÖë
d~íÉï~ó=~ÇÇêÉëë
akp=ëÉííáåÖë
m_u=ëÉííáåÖë
rëÉê=ëÉííáåÖë
cqm=ëÉííáåÖë
si^k=ëÉííáåÖë
si^k=m`=éçêí=ëÉííáåÖ
pfm=ëÉííáåÖë
k^q=ëÉííáåÖë
ptfq`e=ëÉííáåÖë
qlp=î~äìÉ
dÉåÉê~ä=~Çãáå

pÉäÉÅí
```

Go to **SWITCH settings** and press the fox key **Select**.

The following screen is displayed:

```
ZZ=ptfq`e=ëÉííáåÖë=ZZ
m`=mçêí
i^k=éçêí
```

```
pÉäÉÅí
```

Go to **PC Port** and press the fox key **Select**.

- Check on the following screen the value associated with the PC port.

Press **C** to return to the previous menu. Go to **LAN Port** and press the fox key **Select**.

- Check on the following screen the value associated with the LAN port.

**Viewing the negotiation with the WEB interface:**

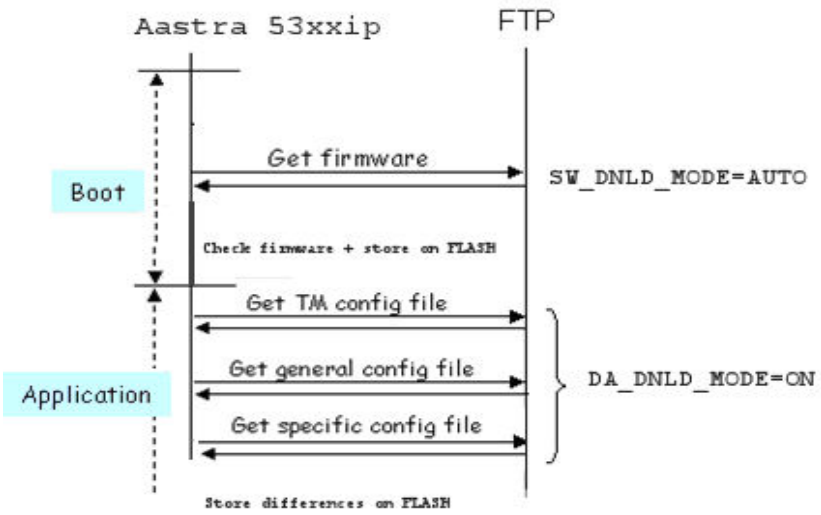
Enter the terminal IP address in the web browser window in http mode (http:// ...),

- Select **Configuration Page**.
- Click the **Switch** tab.

Mitel recommends configuring the ports of Ethernet switches supporting MiVoice 5300 IP Phone in ‘Auto-negotiation’ mode; the same rule applies to the network cards of PCs connected to the terminal.

# 16.4 DOWNLOADING THE FIRMWARE AND CONFIGURATION FILES OF MIVOICE 5300 IP PHONES

## 16.4.1 MIVOICE 5300 IP PHONE DOWNLOADING TOOLS




The MiVoice 5300 IP Phone loading tool consists of two distinct sequences:

- Boot sequence
- Application start sequence.

**Boot sequence:**

When the terminal is first started, it runs the boot sequence. The DHCP mode is activated by default. If it has been deactivated through configuration, no DHCP request is sent by the terminal. From the FTP server IP address defined manually on the terminal, this latter connects to the aamadeus user account of the FTP server and downloads the available firm in the account storage directory, according to the following rules:

The parameter **SW_DNLD_MODE** defines the firmware download policy.

- **AUTO**: the terminal updates its firmware. If the file is not specified **(**aamxip_v*.ftp), the terminal checks all the files whose name has the format aamxip_vX_Y_Z.ftp and updates its firmware with the latest available release.

  If the file is specified (aamxip_vX_Y_Z.ftp), the terminal firmware is only updated if the version available in FLASH is lower than the one specified.

- **FORCED**: the terminal reloads its firmware without taking account of its current version in FLASH.

  This makes it possible to reload the current version, a previous or new version by specifying the name of the firmware to download (aamxip_vX_Y_Z.ftp). At the end of the reload operation, this parameter is automatically reset to AUTO.

- **OFF**: the terminal does not reload its firmware.

**Note : The vX_Y_Z string corresponds to the firmware version.**

**Note : If the firmware contains a new boot version, the terminal updates it and reboots from this new boot version.**

**Application start sequence.**

The application start sequence follows the boot sequence immediately.

The parameter **DA_DNLD_MODE** specifies the configuration file download policy.

- **ON**: the terminal downloads its configuration files automatically.
- **OFF**: the terminal does not download its configuration files.

If the parameter **DA_DNLD_MODE** is set to **ON** (default value), the application tries to download chronologically the following configuration files:

1. **MiVoice 5300 IP Phone initialisation file: tm.config.<TT>.<VN>.ftp**
   - <TT> stands for the terminal model (60ip, 70ip, 80ip).
   - <VN> stands for the version of the "Terminal Model". This value must be consistent with the terminal firmware version (vX_Y_Z).



**ATTENTION : This is a system file that should not be modified for any reason whatsoever. The terminal will not work if the transfer of this file fails.**

2. **Global configuration file: localdb.config.ftp**

This configuration file is used for all MiVoice 5300 IP Phone. Its format is defined in the following chapter. It can be modified by the administrator to configure certain network parameters common to all MiVoice 5300 IP Phones on the installation.

3. **Specific configuration files: localdb.config.<MAC@>.ftp and localdb.config.<TN>.ftp**
   - <MAC@> is the terminal MAC address. The MAC address block for MiVoice 5300 IP Phones always starts with 00085D84xxxx. This information is available at the back of the terminal or in the Status tab of the web interface.
   - <TN> stands for the directory number defined in the USER_PHONE_NUMBER field.

If the USER_PHONE_NUMBER field is empty (default factory setting), the terminal will download the specific file localdb.config.<MAC@>.ftp

If the USER_PHONE_NUMBER field contains a value (terminal has already logged onto the system or a value has been entered manually), the terminal will download the specific file localdb.config.<TN>.ftp. In case of failure, if the file is not available on the FTP server, the terminal will switch over to the specific file localdb.config.<MAC@>.ftp

This file is specific to a MiVoice 5300 IP Phone. Its format is defined in the following chapter. It can be modified by the administrator to configure certain network parameters specific to all MiVoice 5300 IP Phones on the installation.

### 16.4.2 MIVOICE 5300 IP PHONE PARAMETER PRIORITY

The parameters have the following descending order of priorities:

- Parameters stored in the Flash memory during a previous start operation
- Parameters obtained by DHCP during start-up
- Default coded parameters

The parameters saved in flash have been modified through the terminal MMC, using the PBX command via the TMA application, or by downloading some data files.

The terminal backs up the parameters in the flash memory in the following descending order of priorities:

- Parameters provided by a specific data file
- Parameters provided by a general data file
- Parameters obtain via DHCP.

The specific file localdb.config.<TN>.ftp has priority over the specific file localdb.config.<MAC@>.ftp if both files are available and downloaded by the terminal.

**ATTENTION : * Negotiation with option 66 DHCP server is accepted if the flash value in the terminal is the default value (factory configuration) or 0.0.0.0.**

**ATTENTION : * Negotiation with option 67 DHCP server is accepted if the flash value in the terminal is the default value and if the firmware name starts with “aamxip”.**

## 16.4.3 CONFIGURATION FILE FORMAT OF MIVOICE 5300 IP PHONES

### *16.4.3.1 MiVoice 5300 IP Phone global configuration file format*

The format for the global configuration file provided in the example (**localdb.config.ftp)** is as follows:

```
# CFG_GLOBAL_INDEX=0
# index used in the register for Global configuration file
# DHCP_ENABLED=1
# (1:DHCP configuration, 0:static IP addressing)
# IP_ADDRESS=192.168.104.33
# address of the terminal (used only if DHCP_ENABLED = 0)
# GATEWAY=0.0.0.0
# gateway of the terminal (used only if DHCP_ENABLED = 0)
# SUBNET_MASK=255.255.255.0
# subnet mask of the terminal (used only if DHCP_ENABLED = 0)
# DNS_SERVER=0.0.0.0
# used to resolve the address of the PBX (If this setting has the default value (0.0.0.0), no DNS query will be done). This parameter can be set via DHCP Server (option 6)
# DNS_NAME=intelligate
# If this parameter is empty, the terminal doesn’t use DNS but will contact the IP address specified by the field PBX_ADDRESS
# DNS_NAME_BACKUP=
# If this parameter is empty, the terminal doesn’t use DNS but will contact the IP address specified by the field PBX_ADDRESS_BACKUP
# PBX_ADDRESS=0.0.0.0
# iPBX address (if a PBX address is entered manually, clear DNS_NAME to make it effective)
# PBX_ADDRESS_BACKUP=0.0.0.0
# iPBX backup address (if a 2nd PBX address is entered manually, clear DNS_NAME_BACKUP to make it effective)
# ADMIN_PASSWORD=0000
# protects local configuration (via local MMI and Web)
# VLAN_ENABLED=0
# 0:disables VLAN VoIP port tagging (802.1q), 1:enables VLAN VoIP port tagging (802.1q)
# VLAN_ID=0
# Specifies the VLAN ID of the terminal VoIP port
# VLAN_PRIO=0
# Specifies the VLAN priority of the terminal VoIP port
# VLANPC_ENABLED=0
# 0 : disables VLAN for PC Port, 1 : enables VLAN for PC port
# VLANPC_ID=0
# Specifies the VLAN ID of the terminal PC port
# VLANPC_TAGS=0
# Specifies wether the VLAN tags (802.1q) of the terminal PC port should be enabled (1) or disabled (0).
# VLANPC_PRIO=0
# Specifies the VLAN priority of the terminal PC port
# PC_PORT=1
# 0 = off, 1 = auto-negociation, 2 = 100 halfduplex, 3 = 100 fullduplex
# LAN_PORT=1
# 1 = auto-negociation, 2 = 100 halfduplex, 3 = 100 fullduplex
```

```
# SIP_PORT_PBX=18060
# SIP port used by SIP access point (GSI)
# SIP_PORT_PBX_BACKUP=18060
# SIP port used by backup SIP access point (GSI)
# SIP_PORT_PHONE=18060
# SIP port used by the terminal
# NAT_RPORT_ENABLED=0
# 0 = desables NAT public media port (rport), 1 = Uses NAT public media port (rport)
# MEDIA_PORT=30000
# media port (rport)
# DA_DNLD_MODE=1
# controls the download of the configuration files and TM (terminal model) init files (0 = off, 1 = auto)
# SW_DNLD_MODE=1
# controls the Software download (0 = off, 1 = auto, 2 = develop, 3 = forced)
# FTP_SERVER=192.168.104.1
# FTP Server address (FTP server address must be provided by DHCP opt. 66)
# FTP_USER=aamadeus
# FTP_PASSWORD=aamadeus
# FTP_FILENAME=aamxip_v*.ftp
# Filename of the firmware to download on the terminal (filename must be provided by DHCP opt. 67)
# FTP_PORT_SERVER=21
# TOS_VALUE=0
# TOS settings (QoS level 3 : diffserv)
#SIP_TRANS_PROTO=UDP
#TRUSTED_CERTS=ca.crt
#TIME_SERVER=europe.pool.ntp.org
DNS_NAME=
SIP_PORT_PBX=5060
SIP_PORT_PHONE=5060
```



**ATTENTION : The comment lines must have a space after #.**



**ATTENTION : The active lines should not have any space, tables or any other character before the field and after the field value. The active lines must be placed at the end of the file and not in the comment block.**

#### *16.4.3.2 MiVoice 5300 IP Phone specific configuration file format*

The format for the two specific configuration files provided in the (**localdb.config.MAC@.ftp) and (localdb.config.TN.ftp)** is as follows:

```
# CFG_SPECIFIC_INDEX=0
# index used in the register for Specific configuration file
# USER_PHONE_NUMBER=
# phone number of the terminal used for an automatic login
# USER_PASSWORD=
# MD5 password of the terminal
```



**ATTENTION : The file's MAC address field must be in lower case on the LINUX platform, as well as the ftp suffix.**



**ATTENTION : The comment lines must have a space after #.**



**ATTENTION : The active lines should not have any space, tables or any other character before the field and after the field value. The active lines must be placed at the end of the file and not in the comment block.**

# 17 APPENDIX 6: MANUAL CONFIGURATION OF MITEL 6000 SIP PHONES

Manual configuration of Mitel 6000 SIP Phones may be envisaged for implementing some terminals on a single-site Mitel 5000 Gateways system for which the integrated TMA is not used. This solution requires the availability of an integrated or external FTP server. The network parameters required by the terminal to work well are declared manually, either from the terminal or from the WEB interface.

These network parameters can also be configured and downloaded from the FTP server.

In this case, the integrated FTP server IP address, login and password associated with the user account used by Mitel 6000 SIP Phones are the only network parameters that require a manual configuration.

Configuration files are made available manually on the FTP server storage area by the administrator.

## 17.1 DEFAULT CONFIGURATION WHEN THE TERMINAL IS INSTALLED FOR THE FIRST TIME

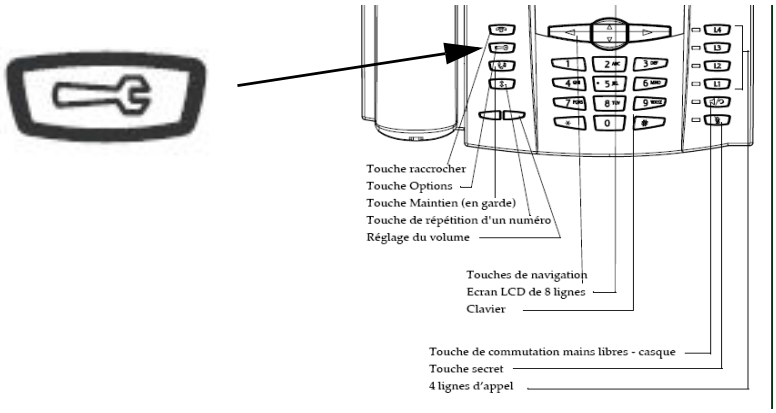
A new terminal has the following factory configuration (default configuration):

- The DHCP option is enabled.
- The terminal's default IP address is: 169.254.114.9
- The default sub-net mask value is: 255.255.255.0
- TFTP is enabled.

## 17.2 MANUAL CONFIGURATION FROM MITEL 6000 SIP PHONES

You can access the manual configuration of the terminal via the "Options" key.

Location of the "Options" key on Mitel 6000 SIP Phones*:




A password is required for the parameters reserved for the administrator.

By default, this password is 22222.

You can choose menus with the navigation key and/or display keys (6755 SIP and 6757 SIP phones).

You can use the UP and DOWN arrow keys to display the different status and text messages on the LCD (if there is more than one status/text message line). You can also use these keys to scroll down the menu options, like the options list.

You can use the LEFT and RIGHT arrows to view the different call lines/functions.

If you are on the options list, you can use these keys to open or exit the current option. If you are editing inputs on the screen, the LEFT arrow deletes the character on the left while the RIGHT arrow confirms the option.

You can use the display keys to directly access a function, for instance, to take account of the parameters of a menu (‘Done’).

To configure each parameter, use the contextual keys:

- "Change": for changing the value or content of a parameter
- "Done": for saving the modification
- "Cancel": for cancelling the modification and returning to the previous menu

**Note : * To access the administration menu of the 6751 SIP phone:**

**Press the Services key.** 

**Select the Options menu.**

**Select an option, by using**  **to browse through the list, or press the number corresponding to the option.**

### 17.2.1 CONFIGURE THE NETWORK SETTINGS OF MITEL 6000 SIP PHONES

- Press the ‘Options’ key.
- In the parameter option list, select: ’Administrator Menu’ then press ’Select’.
- Enter the administrator password (22222) then press ’Enter’ to confirm.
- Select ‘Network Settings’ then press ‘Select’.
- Use the navigation key to access the different network parameters:

1-DHCP

2-IP Address

3-Subnet Mask

4-Gateway

Set the DHCP field to No.

Fill in the fields corresponding to the terminal IP address, subnet mask and gateway (router) IP address.

### 17.2.2 CONFIGURING THE FTP SERVER PARAMETERS OF MITEL 6000 SIP PHONES

- Press the ‘Options’ key.
- In the parameter option list, select: ’Administrator Menu’ then press ’Select’.
- Enter the administrator password (22222) then press ’Enter’ to confirm.
- Select ‘Configuration server’ then press ‘Select’.
- Select ‘’Download protocol’ then press ‘Select’.
- Using the navigation key, select ‘use FTP’ and confirm with the ‘Done’ key.
- In the ‘Configuration Server’ menu, select the parameter ‘FTP Settings’.
- In the ’FTP Server’ menu, enter the FTP server IP address.
- In the ‘FTP Username’ menu, enter the login of the FTP server account used by Mitel 6000 SIP Phones.
- In the ‘FTP Password’ menu, enter the account password.

### 17.2.3 CONFIGURE THE SIP SETTINGS OF MITEL 6000 SIP PHONES.

- Press the ‘Options’ key.
- In the parameter option list, select: ’Administrator Menu’ then press ’Select’.

- Enter the administrator password (22222) then press ’Enter’ to confirm.
- Select ‘SIP Settings’ then press ‘Select’.
- Select ‘Proxy IP/Port’ then press ‘Select’.
  - Enter the SIP access point address (UCV card IP address) and the default port address (5060).
- Select ‘Registar IP/Port’ then press ‘Select’.
  - Enter the SIP access point address (UCV card IP address) and the default port address (5060).
- Select ‘User Name’ then press ‘Select’.
  - Enter the subscription number of the terminal declared in the iPBX.
- Select ‘Display Name’ then press ‘Select’.
  - Enter the name that must be displayed on the requested terminal screen.
- Select ‘Screen Name’ then press ‘Select’.
  - Enter the name that must be displayed on the terminal screen.

**Note : These parameters may be configured in the files aastra.cfg and MAC@.cfg then downloaded to the terminal from the FTP server.**

**ATTENTION : UDP ports 5060 (signal flow) and 40000 (voice flow) must be open on the MiVoice 5000 Server if the firewall is enabled.**

### 17.2.4 DEFINE THE LAN PORT VLAN PARAMETERS OF MITEL 6000 SIP PHONES

- Press the ‘Options’ key.
- In the parameter option list, select: ’Administrator Menu’ then press ’Select’.
- Enter the administrator password (22222) then press ’Enter’ to confirm.
- Select ‘Network Settings’ then press ‘Select’.
- Select ‘VLAN Settings’ then press ‘Select’.
- Select ‘VLAN Enable’ and set the value to Yes to authorise frame marking.
- Select ‘LAN port VLAN’ then ‘LAN port VLAN ID’ and set the ToIP VLAN value.
- Select the ‘VLAN priority’ and set the value of the priority associated with the ToIP VLAN for signal (SIP) and audio (RTP) flows.

**Note : These parameters may be configured in the files aastra.cfg then downloaded to the terminal from the FTP server.**

### 17.2.5 DEFINE THE PC PORT VLAN PARAMETERS OF MITEL 6000 SIP PHONES

- Press the ‘Options’ key.
- In the parameter option list, select: ’Administrator Menu’ then press ’Select’.
- Enter the administrator password (22222) then press ’Enter’ to confirm.
- Select ‘Network Settings’ then press ‘Select’.
- Select ‘VLAN Settings’ then press ‘Select’.
- Select ‘PC port VLAN’ then ‘PC port VLAN ID’ and set the Data VLAN value.
- Select ‘PC port priority’ then set the priority value associated with the Data VLAN.

**Note : These parameters may be configured in the files aastra.cfg then downloaded to the terminal from the FTP server.**

### 17.2.6 RESTART THE MITEL 6000 SIP PHONES

- Press the ‘Options’ key.
- From the options list, select the parameter ‘Restart Phone’ and press ‘Select’.
- Confirm the restart operation by selecting and pressing ‘Restart’.

The terminal restarts, taking account of the previously modified parameters. This will enable it to connect to the FTP server and to download the firmware, configuration files and language packs available in the server storage area.

### 17.2.7 CONFIGURE MITEL 6000 SIP PHONES IN FRENCH LANGUAGE:

**Note : The languages are available in the ‘languages pack’ and must be downloaded to the terminal for use. They can be downloaded from the FTP server, either by restarting the terminal manually, or by programming automatic update via the parameter Auto-Resync in Menu "Advanced settings > Configuration server’"**

- Press the ‘Options’ key.
- From the options list, select the parameter ‘Preferences’ and press ‘Select’.
- In the ‘Preferences’ menu, select ‘Language’ then press ‘Select’.
- In the ‘Language’ menu, select ‘Screen Language’ then press ‘Select’.
  - Change the language with the navigation key then confirm the selection with the ‘Done’ key.
- In the ‘Language’ menu, select ‘Input Language’ then press ‘Select’.
  - Change the language with the navigation key then confirm the selection with the ‘Done’ key.

## 17.3 MANUAL CONFIGURATION OF MITEL 6000 SIP PHONES VIA THE WEB INTERFACE

First define the terminal IP address via the terminal interface.

Connect via a WEB browser: http://@IP_poste_A6xxxi

- Access in User mode:
  - Username: user
  - Password: 10/11111
- Access in Administrator mode:
  - Username: admin
  - Password: 10/22222

### 17.3.1 CONFIGURING THE BASIC NETWORK SETTINGS OF MITEL 6000 SIP PHONES

Procedure:

- Connect as Administrator.
- In Menu ‘Advanced settings > Network’, disable DHCP mode to automatically obtain an address and enter manually the IP address, subnet mask and default gateway of Mitel 6000 SIP Phone.
- Confirm your modifications by clicking <Save settings>.

### 17.3.2 CONFIGURING THE FTP SERVER FOR MITEL 6000 SIP PHONES

The terminals’ firmware release and configuration files are made available, by default, in the FTP server storage directory integrated into the system’s UCV card.

This window allows you to enter the IP address of an FTP server so as to download files to the terminal (for updating the firmware, configuration files, and language packs).

Procedure:

- Connect as Administrator.
- In the menu ‘Advanced settings > Configuration server’, select FTP in the ‘Download protocol’ field.
- Enter the FTP server IP address as well as the login and associated password.

**Note :** **Note :By default, the login and password defined on the FTP server incorporated into Mitel 5000 Gateways for Mitel 6000 SIP Phone are:**
**login: ftp_67xxi**
**Password: ftp_67xxi**

- Confirm your modifications by clicking "Save settings".

### 17.3.3 CONFIGURING THE SIP SETTINGS OF MITEL 6000 SIP PHONES

This window allows you to define the terminal's global settings. The basic settings are:

- 'Screen Name' and 'Screen Name 2': name displayed on the terminal screen
- 'Phone number': terminal subscription number
- 'Proxy Server'/ 'Registrar Server': SIP access point IP address
- 'Proxy Port' / 'Registrar Port': use the standard value 5060.
- 'Registration Period': use the standard value 3600 (1h)

Procedure:

- Connect as Administrator.
- In Menu 'Advanced settings > global SIP', enter the parameters described above.
- Confirm your modifications by clicking <Save settings>.

**Note : These parameters may be configured in the files aastra.cfg and MAC@.cfg then downloaded to the terminal from the FTP server.**

### 17.3.4 RESTART THE MITEL 6000 SIP PHONES

Procedure:

- Connect as Administrator.
- In Menu 'Operation > Reset', click 'Restart Phone'.

The terminal restarts, taking account of the previously modified parameters. This will enable it to connect to the FTP server and to download the firmware, configuration files and language packs available in the server storage area.

### 17.3.5 CONFIGURING THE WEB INTERFACE LANGUAGE

To change the web interface language:

- Connect as Administrator.
- In Menu 'Basic Settings > Preferences', select the language of your choice from those available in the parameter 'Webpage Language':
  - English
  - French
  - German
  - Italian
  - Spanish
- Confirm your modifications by clicking <Save settings>.

**Note : The languages are available in the 'languages pack' and must be downloaded to the terminal for use. They can be downloaded from the FTP server, either by restarting the terminal manually, or by specifying the name of the language file to use. Programming an automatic update via the parameter Auto-Resync in the menu 'Advanced settings > Configuration server' automates this downloading operation.**

### 17.3.6 DOWNLOADING A LANGUAGE PACK ON MITEL 6000 SIP PHONES

A language pack can be downloaded to Mitel 6000 SIP Phone in two ways:

- Via the file aastra.cfg
- Via the web interface

Downloading via the file aastra.cfg

You can use the configuration file aastra.cfg to specify the language pack to download using the following format:

lang_<ISO 639>-<ISO 3166>.txt ou lang_<ISO 639>.txt where <ISO 639> is the language code specified in standard ISO 639 and <ISO 3166> is the country code specified in standard ISO 3166.

ISO <3166> is an optional attribute.

The addition or modification of a language pack is only taken into account when the terminal is restarted. The default language (English) can neither be modified nor deleted.

The following example describes the default configuration made in the file aastra.cfg to download the language packs French, Italian, German and Spanish to Mitel 6000 SIP Phones.

language 1: lang_fr.txt # French language file name

language 2: lang_de.txt # German language file name

language 3: lang_it.txt # Italian language file name

language 4: lang_es.txt # Spanish language file name

Via the web interface

- Connect as Administrator.
- In the menu ‘Basic Settings > Preferences > Language Settings’, enter the language pack to download in language fields 1 to 4:
  - lang_fr.txt
  - lang_de.txt
  - lang_it.txt
  - lang_es.txt
- Confirm your modifications by clicking <Save settings>.



**ATTENTION : You have to restart the terminal for the downloaded language pack to be taken into account.**

# 17.4 CONFIGURING ETHERNET SWITCHES FOR MITEL 6000 SIP PHONES

## 17.4.1 REMOTE SUPPLY TO MITEL 6000 SIP PHONES

Mitel 6000 SIP Phone are PoE compatible (802.3af), except the 6730 SIP model which requires a 5V/ 2A mains unit.

## 17.4.2 MODES SUPPORTED BY THE TERMINAL'S INTEGRATED SWITCH PORTS

The ports of Mitel 6000 SIP Phones support the following three transmission modes:

- Auto-negotiation
- Half-duplex (10Mb/s or 100 Mb/s)
- Full-duplex (10Mb/s or 100 Mb/s)

Viewing the result of the negotiation on the terminal

Press the 'Options' key and select 'Phone Status'.

To view the LAN port status:

In the 'Phone status' menu, select 'LAN port' then press 'Select'.

To view the PC port status:

In the 'Phone status' menu, select 'PC port' then press 'Select'.

Viewing the negotiation with the WEB interface:

Mitel recommends configuring the ports of Ethernet switches supporting Mitel 6000 SIP Phones in 'Auto-negotiation' mode; the same rule applies to the network cards of PCs connected to the terminal.

# 17.5 DOWNLOADING THE FIRMWARE AND CONFIGURATION FILES OF MITEL 6000 SIP PHONES

## 17.5.1 MITEL 6000 SIP PHONE DOWNLOADING TOOLS

By default (factory settings), Mitel 6000 SIP Phones are set to DHCP and use TFTP to load the firmware and configuration files. The configuration needs to be modified for the MiVoice 5000 range in order to indicate to Mitel 6000 SIP Phone to use FTP. This modification is either made manually from the web interface or from the terminal, or automatically via option 43 or 66 which can be used with a DHCP server.

The protocols available for downloading are: TFTP, FTP, HTTP and HTTPS

The downloading server hosts the terminals' firmware, configuration files and language packs.

Format of files used for downloading:

- Firmware: <terminal type>.st (example: 55i.st)
- Terminal global configuration file: **aastra**.cfg
- Terminal-specific configuration file: @MAC.cfg (example: 00085D3A2451.cfg)
- language pack files: lang_<ISO 639>_<ISO 3166>.txt or lang_<ISO 639>.txt (ex: lang_fr_ca.txt or lang_de.txt).



**ATTENTION : Combining the different methods may lead to configuration clashes, and unexpected behaviour of the terminal.**



**ATTENTION : All the file names must be entered in lower case, except the '@MAC' field which must be entered in upper case (see examples above).**

When the terminal is started, it checks on the FTP server for file updates and downloads them if necessary. The terminal downloads the beginning of the firmware and compares it to what it already has in flash before continuing with the download if the terminal version is lower that the firmware to download. The configuration files and language packs are systematically downloaded.

Reload policy

Reloading always takes place after the terminal is restarted. This terminal restart may be requested, directly on the terminal, remotely via the web interface or automatically by the terminal at a specific time everyday, or automatically by the iPBX via the TMa application. Automatic download at specific time may be inhibited.



**ATTENTION : Manual update of the Mitel 6000 SIP Phone firmware is not available from an FTP server, but only from a TFTP server.**

## 17.5.2 MITEL 6000 SIP PHONE PARAMETER PRIORITY

The parameter values are applied in the following order (1 is the highest priority level):

1. Parameters obtained via the iPBX through NOTIFY messages (parameters configuration menu for the Mitel 6000 SIP Phones of Web Admin),
2. Parameters obtained via the TMA (FTP server address and account to use)
3. Parameters obtained via the DHCP server
4. Parameters configured manually (from the web interface or terminal)
5. Parameters obtained by the specific configuration file via the FTP server
6. Parameters obtained by the global configuration file via the FTP server
7. Default parameters in the terminal (factory settings)

Example:

If the terminal language is configured:

In "Italian" in the specific configuration file @MAC.cfg

In "French" via the terminal's MMI

In "English" in the global configuration file aastra.cfg

After the terminal is restarted, it will be set to French, since the manually configured parameters have the highest priority level.

## 17.5.3 MITEL 6000 SIP PHONE SPECIFIC CONFIGURATION FILE FORMAT

### *17.5.3.1 Mitel 6000 SIP Phone global configuration file format*

The configuration file aastra.cfg configures the data used by all Mitel 6000 SIP Phone.

The data below is communicated as an example and presents most of the parameters of the Mitel 6000 SIP Phones to configure for the MiVoice 5000 solution.

This file must be reviewed for each installation based on the need.

Some parameters must retain the default value for the MiVoice 5000 solution, as indicated below.

```
# ----------------------------------------
#aastra.cfg
#
# File created on 01/10/2010 14:44:01
#
# ----------------------------------------
# The proxy server's port number / THIS PARAMETER MUST BE UNCHANGED
sip proxy port: 10/5060
# The registrar's port number / THIS PARAMETER MUST BE UNCHANGED
sip registrar port: 10/5060
# The backup proxy server's port number / THIS PARAMETER MUST BE UNCHANGED
sip backup proxy port: 10/5060
# The backup registrar's port number / THIS PARAMETER MUST BE UNCHANGED
sip backup registrar port: 10/5060
# Download protocol / THIS PARAMETER MUST BE UNCHANGED
download protocol: FTP
# Activating the line at the numbering ML / THIS PARAMETER MUST BE UNCHANGED
live dialpad: 10/1
# Web interface enabled 1= yes, 0=no
web interface enabled: 10/1
# Allows you to specify a timeout value, in seconds, that the phone waits for the far side to return a response after accepting the HTTP GET connection
xml get timeout: 10/12
```

# Enables or disables the use of "directed call pickup" feature / THIS PARAMETER MUST BE UNCHANGED
directed call pickup: 10/1
# Specifies the time period, in seconds, that the IP phone resubscribes the BLF subscription service after a software/firmware upgrade or after a reboot of the IP phone. / THIS PARAMETER MUST BE UNCHANGED
sip blf subscription period: 10/3600
# Tones choice by country (Australia, Europe, France, Germany, Italy, Mexico, UK, US)
tone set: France
# Enables or disables the ability to initiate a continuous reminder tone in the active call when another call is on hold
call hold reminder during active calls: 10/0
# Enables or disables ring splash timer to start as soon as you put a call on hold
call hold reminder: 10/0
# Specifies a time delay in seconds that a ring splash is heard on a active call when another call was placed on hold
call hold reminder timer: 10/0
# Specifies the time interval, in seconds, between each ring splash sound on the active call
call hold reminder frequency: 10/0
# Allows you to specify the language to use for inputs on the IP Phone
input language: French
# File name for the language 1
language 1: lang_fr.txt
# File name for the language 2
language 2: lang_de.txt
# File name for the language 3
language 3: lang_it.txt
# File name for the language 4
language 4: lang_es.txt
# The language you want to display in the IP Phone UI and the aastra Web U 0 (English) 1(French) 2 (Spanish) 3 (German) 4 (Italian)
language: 10/1
# language by default on the WEB page (1=French, put in comment to have the english configuration)
web language: 10/1
# 0 (WWWW MMM DD) 1 (DD-MMM-YY) 2 (YYYY-MM-DD) 3 (DD/MM/YYYY) 4 (DD/MM/YY) 5 (DD-MM-YY) 6 (MM/DD/YY) 7 (MMM DD) 8 (DD MM YYYY) 9 (WWW DD MMM) 10 (DD MMM) 11 (DD.MM.YYYY)
date format: 10/9
# 0 = 12 hour format, 1 = 24 hour format
time format: 10/1
# 0 = hour management by NTP serveur, 1 = Unactivated / THIS PARAMETER MUST BE UNCHANGED
time server disabled: 10/0
# time server's IP address
time server1: 192.168.65.1
# Assigns a time zone code to the time server
time zone code: CET
# Assigns a time zone name to the time server
time zone name: Dublin -UK
# DHCP = 1 : enabled on A 5000.
dhcp: 10/1
# Enables or disables VLAN on the IP phones
tagging enabled: 10/0
# Specifies the VLAN ID used to pass packets through to a PC via Port 1
VLAN id port 1: 10/4095
# On the IP phone, you configure a VLAN ID that associates with the physical Ethernet Port 0
VLAN id: 10/21
# Enables or disables Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) on the IP Phone
lldp: 10/0
# Allows you to enable or disable a dial plan terminator / THIS PARAMETER MUST BE UNCHANGED
sip dial plan terminator: 10/0
# Emergency number
emergency dial plan: "018|015|017|0112|11x|18|17|15"
# Sets the Dual-tone multifrequency (DTMF) method to use on the IP phone
sip dtmf method: 10/1
# Enables or disables out-of-band DTMF

sip out-of-band dtmf: 10/0
# Sending of silence DTMF
suppress dtmf playback: 10/1
# Specifies a customized Codec preference list which allows you to use the preferred Codecs for this IP phone. / THIS PARAMETER MUST BE UNCHANGED
sip customized codec:
payload=8;ptime=20;silsupp=off,payload=0;ptime=20;silsupp=off,payload=18;ptime=20;silsupp=off,payload=18;ptime=40;silsupp=off
# Enables or disables basic codecs / THIS PARAMETER MUST BE UNCHANGED
sip use basic codecs: 10/0
# Enables or disables the microphone on the IP phone for Intercom calls made by the originating caller / THIS PARAMETER MUST BE UNCHANGED
sip intercom mute mic: 10/0
# indicator of message (Led) 1=activated, 0=unactivated
sip explicit mwi subscription: 10/1
# Enables or disables the ability to configure Call Forwarding / THIS PARAMETER MUST BE UNCHANGED
call forward disabled: 10/1
# Allows to specify which key types to display / THIS PARAMETER MUST BE UNCHANGED
softkey selection list: none, line, speeddial, blf, xml, directory, callers, conf, xfer, services, phonelock, empty
# Enables or disables dnd softkey under service key on 39i / THIS PARAMETER MUST BE UNCHANGED
dnd ui: 10/0
# blind forward method
sip cancel after blind transfer: 10/1
# the phone handles incoming calls while the phone is dialing out
incoming call cancels dialing: 10/1
# / THIS PARAMETER MUST BE UNCHANGED
dynamic sip: 10/1
# / THIS PARAMETER MUST BE UNCHANGED
rtp hardlock: 10/1
# / THIS PARAMETER MUST BE UNCHANGED
sip aastra id: 10/1
# / THIS PARAMETER MUST BE UNCHANGED
sip accept out of order requests: 10/1
# / THIS PARAMETER MUST BE UNCHANGED
sip forward mode: 10/0
# Specifies the local source port (UDP/TCP) from which the phone sends SIP messages / THIS PARAMETER MUST BE UNCHANGED
sip local port: 10/5060
# Specifies the local source port (SIPS/TLS) from which the phone sends SIP messages / THIS PARAMETER MUST BE UNCHANGED
sip local tls port: 10/5061
# Allows you to configure the mode of the line. Applicable values are 0 - Generic, 1 - BroadSoft SCA 2- Nortel, 3 - BLA / THIS PARAMETER MUST BE UNCHANGED
sip mode: 10/0
# Adds an aastra-Line: header to the SIP REGISTER messages sent from the phone to the call server, where the value is the MAC address of the phone / THIS PARAMETER MUST BE UNCHANGED
sip send line: 10/1
# The phone negotiates whether or not to use silence suppression: enable (1) or disable (0) . / THIS PARAMETER MUST BE UNCHANGED
sip silence suppression: 10/0
# Enables or disables the phone to accept or reject an aastra-xml SIP NOTIFY message / THIS PARAMETER MUST BE UNCHANGED
sip xml notify event: 10/1
# Allows you to enable (1) or disable (0) the use of Rport on the IP phone / THIS PARAMETER MUST BE UNCHANGED
sip rport: 10/0
# use TLS (4), UDP (1), TCP (2) or both UDP and TCP (0) for sip messaging / THIS PARAMETER MUST BE UNCHANGED
sip transport protocol: 10/1
# Enables (1) or disables (0) the use of Persistent Transport Layer Security / THIS PARAMETER MUST BE UNCHANGED
sips persistent tls: 10/0
# Disable (0) or enable (1)
sips tls authentication: 10/0
# 0 (SRTP Disabled) 1 (SRTP Preferred) 2 (SRTP Only) / THIS PARAMETER MUST BE UNCHANGED
sip srtp mode: 10/0

# Enables or disables Globally Routable User-Agent URI (GRUU) / THIS PARAMETER MUST BE UNCHANGED
sip gruu: 10/1
# This parameter is based on the Type of Service (ToS),Differentiated Services Code Point (DSCP) setting for SIP (tos sip parameter), RTP (tos rtp parameter) and RTCP (tos rtcp parameter). It is the mapping between the DSCP value and the VLAN priority value for SIP, RTP, and RTCP packets
tos priority map: (40,5)(46,5)
# The Differentiated Services Code Point (DSCP) for RTCP packets
tos rtcp: 10/46
# The Differentiated Services Code Point (DSCP) for RTP packets
tos rtp: 10/46
# The Differentiated Services Code Point (DSCP) for SIP packets
tos sip: 10/40
# Enables or disables the https validation of certificates on the phone (0 : disabled, 1 : enabled) / THIS PARAMETER MUST BE UNCHANGED
https validate certificates: 10/0
# Parameter required for validation robot
enable atap: 10/32791
# Allows you to lock or unlock the Save key on the 6753iIP Phone (0=unlock, 1=lock) / THIS PARAMETER MUST BE UNCHANGED
prgkey1 locked: 10/0
# Allows you to lock or unlock the Delete key on the 6753i IP Phone (0=unlock, 1=lock) / THIS PARAMETER MUST BE UNCHANGED
prgkey2 locked: 10/0
# Allows you to lock or unlock the Save key on the 6730/1i IP Phone (0=unlock, 1=lock) / THIS PARAMETER MUST BE UNCHANGED
prgkey5 locked: 10/0
# Allows you to lock or unlock the Delete key on the 6730/1i IP Phone (0=unlock, 1=lock) / THIS PARAMETER MUST BE UNCHANGED
prgkey6 locked: 10/0
# Type of programmation / THIS PARAMETER MUST BE UNCHANGED
prgkey7 type: none
# Type of programmation / THIS PARAMETER MUST BE UNCHANGED
prgkey8 type: none
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey1 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey2 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey3 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey4 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey5 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey6 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey7 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey8 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey9 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey10 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey11 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey12 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey13 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey14 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey15 type: empty

# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey16 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey17 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey18 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey19 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey20 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey21 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey22 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey23 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey24 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey25 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey26 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey27 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 67xxi / THIS PARAMETER MUST BE UNCHANGED
softkey28 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey29 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey30 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey31 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey32 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey33 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey34 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey35 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey36 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey37 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey38 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey39 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey40 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey41 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey42 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey43 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey44 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED

softkey45 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey46 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey47 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey48 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey49 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey50 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey51 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey52 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey53 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey54 type: empty
# Type of programmation. Only effective for 55i, 57i and 39i. No effect on other 6xxi / THIS PARAMETER MUST BE UNCHANGED
softkey55 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key1 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key2 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key3 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key4 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key5 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key6 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key7 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key8 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key9 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key10 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key11 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key12 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key13 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key14 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key15 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key16 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key17 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key18 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key19 type: empty

# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key20 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key21 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key22 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key23 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key24 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key25 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key26 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key27 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key28 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key29 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key30 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key31 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key32 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key33 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key34 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key35 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key36 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key37 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key38 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key39 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key40 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key41 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key42 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key43 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key44 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key45 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key46 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key47 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key48 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED

expmod1 key49 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key50 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key51 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key52 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key53 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key54 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key55 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key56 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key57 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key58 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key59 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod1 key60 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key1 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key2 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key3 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key4 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key5 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key6 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key7 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key8 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key9 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key10 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key11 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key12 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key13 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key14 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key15 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key16 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key17 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key18 type: empty

# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key19 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key20 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key21 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key22 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key23 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key24 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key25 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key26 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key27 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key28 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key29 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key30 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key31 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key32 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key33 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key34 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key35 type: empty
# Type of programmation on expansion module 1 / THIS PARAMETER MUST BE UNCHANGED
expmod2 key36 type: empty

#### 17.5.3.2 Mitel 6000 SIP Phone specific configuration file format

This configuration file '@MAC.cfg' is used for data specific to each terminal.

The specific parameters of a terminal will generally be:

- The name displayed on the terminal's screen
- The subscription number for each terminal line
- The key programming.



**ATTENTION : The file's @MAC field must be in upper case on a LINUX platform, and the suffix cfg in lower case.**

The data below is communicated as an example and presents most of the parameters of the Mitel 6000 SIP Phones to configure for the MiVoice 5000 solution. This file must be reviewed for each installation based on the need.

**Files MAC_30i.cfg and MAC_31i.cfg:**

```
#
# 6731i.cfg
#
#_____________________________________________________________________________
#  Template file
#
# Last update :  <10/09/2009>
#_____________________________________________________________________________
#
# This file"6731i.cfg" contains the key programming made on  6731 SIP phones via TMA menu "Template management".
# LesThe data below is communicated as examples.
# This file will be customised according to the specific characteristics of the installation.
# For a parameter to be active (inactive), remove (put) the character '#' at the beginning of the line.
#
# The file "6731i.cfg" configures keys programmation for 6731 SIP sets. This programmation is done via TMA by using menu "Template management"
# The following data are several examples.
# This file will be customized depending on the specific characteristics of the installation.
# To enable (disable) a parameter, withdraw (put) the number sign (#) at the beginning of the line.
#
#<10/09/2009> : creation
#_____________________________________________________________________________
#
#_____________________________________________________________________________
# Programming personal Programmable Keys
#_________________________
#
#prgkey1 type: speeddial
#prgkey1 value: 10/4302
#prgkey1 locked: 10/1

# Call by name
#prgkey2 type: xml
#prgkey2 value: http://192.168.65.1/directory/i5xi.php
#prgkey2 locked: 10/1

prgkey3 type: dnd
prgkey3 locked: 10/1
```

**File MAC_53i.cfg:**

```
#
# 6753i.cfg
#
#_____________________________________________________________________________
#  Template file
#
# Last update :  <10/09/2009>
#_____________________________________________________________________________
#
# This file "6753i.cfg" contains the key programming made on  6753 SIP phones via TMA menu "Template management".
# LesThe data below is communicated as examples.
# This file will be customised according to the specific characteristics of the installation.
# For a parameter to be active (inactive), remove (put) the character '#' at the beginning of the line.
#
# The file "6753i.cfg" configures keys programmation for 6753i sets. This programmation is done via TMA by using menu "Template management"
# The following data are several examples.
# This file will be customized depending on the specific characteristics of the installation.
# To enable (disable) a parameter, withdraw (put) the number sign (#) at the beginning of the line.
#
#<10/09/2009> : creation
#_____________________________________________________________________________
#

#_____________________________________________________________________________
# Programming personal Programmable Keys
#_________________________
#
# Call by name
#prgkey3 type: xml
#prgkey3 value: http://192.168.65.1/directory/i5xi.php
#prgkey3 locked: 10/1

#prgkey4 type: speeddial
#prgkey4 value: 10/4304
#prgkey4 locked: 10/1

prgkey5 type: dnd
prgkey5 locked: 10/1
```

**File MAC_55i.cfg:**

```
#
# 6755i.cfg
#
#_____________________________________________________________________________
#  Template file
#
# Last update :  <10/09/2009>
#_____________________________________________________________________________
#
# This file "6755i.cfg" contains the key programming made on  6755i phones via TMA menu "Template management".
# LesThe data below is communicated as examples.
# This file will be customised according to the specific characteristics of the installation.
# For a parameter to be active (inactive), remove (put) the character '#' at the beginning of the line.
#
# The file "6755i.cfg" configures keys programmation for 6755i sets. This programmation is done via TMA by using menu "Template management"
```

```
# The following data are several examples.
# This file will be customized depending on the specific characteristics of the installation.
# To enable (disable) a parameter, withdraw (put) the number sign (#) at the beginning of the line.
#
#<10/09/2009> : creation
#_____________________________________________________________________________
#
#_____________________________________________________________________________
# Programming common Programmable Keys
#_____________________

prgkey1 type: directory
prgkey1 locked: 10/1

prgkey2 type: callers
prgkey2 locked: 10/1

prgkey3 type: services
prgkey3 locked: 10/1

prgkey4 type: dnd
prgkey4 locked: 10/1

#prgkey5 type: xml
#prgkey5 line: 10/1
#prgkey5 value: http://192.168.65.1/directory/i5xi.php
#prgkey5 locked: 10/1

#_____________________________________________________________________________
# Programming common Softkeys
#_____________________

#softkey1 type: speeddial
#softkey1 label: Jean Durand
#softkey1 value: 10/4300
#softkey1 line: 10/1

#softkey2 type: speeddial
#softkey2 label: Forward-VMAIL
#softkey2 value: *214450
#softkey2 line: 10/1

#softkey3 type: speeddial
#softkey3 label: Cancel-forw
#softkey3 value: "#20"
#softkey3 line: 10/1
```

**File MAC_57i.cfg:**

```
#
# 6757i.cfg
#
#_____________________________________________________________________________
#  Template file
#
# Last update :  <10/09/2009>
#_____________________________________________________________________________
#
```

```
# This file "6757i.cfg" contains the key programming made on  6757 SIP phones via TMA menu "Tem-
plate management".
# LesThe data below is communicated as examples.
# This file will be customised according to the specific characteristics of the installation.
# For a parameter to be active (inactive), remove (put) the character '#' at the beginning of the line.
#
# The file "6757i.cfg" configures keys programmation for 6757i sets. This programmation is done via
TMA by using menu "Template management"
# The following data are several examples.
# This file will be customized depending on the specific characteristics of the installation.
# To enable (disable) a parameter, withdraw (put) the number sign (#) at the beginning of the line.
#
#<10/09/2009> : creation
#_____
#
#_____
# Programming and locking common Top Softkeys
#_____
#
topsoftkey1 type: directory
topsoftkey1 locked: 10/1

topsoftkey2 type: callers
topsoftkey2 locked: 10/1

topsoftkey3 type: services
topsoftkey3 locked: 10/1

topsoftkey4 type: dnd
topsoftkey4 locked: 10/1

#topsoftkey5 type: xml
#topsoftkey5 line: 10/1
#topsoftkey5 value: http://192.168.65.1/direectory/i5xi.php
#topsoftkey5 locked: 10/1

#_____
# Programming common Bottom Softkeys
#_____

#softkey1 type: speeddial
#softkey1 label: Jean Durand
#softkey1 value: 10/4300
#softkey1 line: 10/1

#softkey2 type: speeddial
#softkey2 label: Forward-VMAIL
#softkey2 value: *214450
#softkey2 line: 10/1

#softkey3 type: speeddial
#softkey3 label: Cancel-forw
#softkey3 value: "#20"
#softkey3 line: 10/1
```

Mitel
Powering connections
mitel.com

© Copyright 2015, Mitel Networks Corporation. All Rights Reserved. The Mitel word and logo are trademarks of Mitel Networks Corporation. Any reference to third party trademarks are for reference only and Mitel makes no representation of ownership of these marks.